A Survey on Cybercrime Using Social Media

Zainab Khyioon Abdalrdha[1]
[1]Iraqi Commission for Computers and Informatics / Informatics Institute of Postgraduate Studies
Baghdad-Iraq
phd202120695@iips.icci.edu.iq

Prof. Dr. Abbas Mohsin Al-Bakry[2]
[2]University of Information Technology and Communication (UoITC)
Baghdad-Iraq
abbasm.albakry@uoitc.edu.iq

Prof. Dr. Alaa K. Farhan [3]
[3]Department of Computer Sciences
University of Technology
Baghdad-Iraq
110030@uotechnology.edu.iq

***Abstract*—There is growing interest in automating crime detection and prevention for large populations as a result of the increased usage of social media for victimization and criminal activities. This area is frequently researched due to its potential for enabling criminals to reach a large audience. While several studies have investigated specific crimes on social media, a comprehensive review paper that examines all types of social media crimes, their similarities, and detection methods is still lacking. The identification of similarities among crimes and detection methods can facilitate knowledge and data transfer across domains. The goal of this study is to collect a library of social media crimes and establish their connections using a crime taxonomy. The survey also identifies publicly accessible datasets and offers areas for additional study in this area**

Keywords: Cybercrime, Deep learning, Crime detection, Social media, Natural Language Processing (NLP).

1. Introduction

Social media is being used for a variety of activities, but can also lead to cybercrime [1]. Online sharing of personal information can lead to crime. Victims may be reluctant to report crimes due to triviality, embarrassment, or lack of awareness. Social media monitoring can be used to augment conventional crime reporting. Social media is being used to facilitate criminal activity, much like other emerging technologies and communication channels [2]. It is imperative to protect private data being transferred via networks [3]. Twitter allows users to share news, thoughts, and ideas in 280 characters, making it unique from other social media forms. Text relationships are not shared in the same way as tweets [4] [5]. Twitter is a popular platform for exchanging data related to cyber threats such as data dumps, security breaches, ransomware, vulnerabilities, DDoS, and zero-day exploits, as well as public events [6]. Researchers may gauge interest in particular topics and identify unanticipated cyber risks in real time with the aid of Twitter's ability to track and send tweets [7]. Security intelligence uses artificial intelligence to collect and organize data concerning cyber threats [8]. To identify criminal traits and concentrate on real-time detection of potential attacks [9]. This necessitates thoroughly detecting and examining both criminal behavior patterns and trends [10]. Communication and technology enable people to perform tasks more quickly and accurately, but they also come with the negative consequence that data transmission is increasingly susceptible to trouble tapping [11]. Twitter tweet classification has also been done using deep learning (DL) based classifiers [12], [13], and [14]. Deep learning like CNN is frequently utilized in this field, and natural language processing techniques are used to analyze language aspects for specific purposes [15]. The similarity in the methods used to commit crimes on social media suggests that techniques used to detect and prevent one type of crime could be applied to other similar crimes. This allows for quick adaptation to new and emerging crimes. This survey paper provides a unique perspective compared to previous papers, which concentrated on particular categories of social media crimes, as it intends to offer a complete summary of how social media is utilized to commit, identify, and anticipate different forms of crimes. The main objectives of this paper include establishing a connection between social media information and crime, consolidating the extensive research in this field, identifying current research trends, documenting relevant resources like datasets, categorizing social media into related groups based on the types of crimes committed, and offering recommendations for future research in this area. We explained in detail the Twitter platform in the introduction and we will briefly explain the rest of the social platforms such as Facebook, and Instagram.

Facebook: the most popular social networking site is Facebook. Facebook's goal is to enable individuals to share and enhance global connectivity, according to the company's website. Facebook gives users the opportunity to upload and share information such as photos and status updates, as well as connect with friends, family, and acquaintances. The platform, which was founded in 2004, has more than 1 billion daily active users and more than 1.65 billion active monthly users. Most of these individuals use it through mobile devices [16]**.** Facebook use is habitual and ritualized, with nearly three-quarters of Internet users having a Facebook account and 7 in 10 users using it daily [17]. Young adults' Facebook usage declined, but adult Internet users still use it [16].

Instagram: This is a photo-sharing mobile application that enables users to take photos, modify them with filters, and post them to Instagram as well as other platforms such as Facebook and Twitter. According to the company's website, Instagram has more than 400 million monthly active users who have posted more than 40 billion photos and garners an average of 3.5 billion likes per day for the more than 80 million photos posted per day on the platform. The majority of Instagram users are young adults (18-29 years old), who report using the app in more than half of the cases [17]. While there are other social media platforms outside of Facebook, Twitter, and Instagram, such as Telegram, YouTube, TikTok, and others, our research focused on three categories of cybercrime.

1.2. Review papers currently available on the subject.

While there has been a significant amount of research on crime and social media, most survey papers have focused on specific offenses like cyberbullying or terrorism-related tweets. A comprehensive survey exploring social media's use in different crimes and their relationships is still lacking. However, since they share similarities, existing crime detection techniques can be adapted to new situations and crimes.

1.3. Paper Structure

The paper is structured into ten distinct parts. The first part introduces the topic, The second part is a literature survey, the third part presents the impact of social media on cybercrime, The fourth part offers a type of cybercrime, and the fifth part offers a comparison of cybercrime occurrences on social media platforms and how they are detected. The sixth part offers comparisons of crime intelligence tools used in social media crimes, The seventh part discusses the results of a study and its future, the eighth part is preventive procedures and Protection mechanisms for cyber crimes In social media, The nine-part offers data set availability and finally, the ten-part summarizes the paper's findings and offers suggestions for future research in this area.

2. Literature Survey

M. M. Islam et al [18] suggested a method for identifying online bullying and abusive messages by combining machine learning and NLP techniques in their paper. In their paper, Aditi, Parth, et al [19], created a system that uses tweets from Twitter to identify terrorist acts by analyzing tweets related to terrorist attacks. By extracting minimal data from Twitter accounts, training detection models, and presenting detection results, Nan Sun and colleagues [20] proposed a system for identifying Twitter spam in almost real time. They aimed to overcome the time lag in data acquisition and spam detection by using features based on both account and content to aid in spam detection. The author Sr. C M proposes in their paper [21] the prediction of major social media crimes by analyzing Twitter data. The study aims to recognize individuals who may commit crimes and predict someone's emotions through social media data analysis. S.P. Sandagiri and colleagues proposed in their paper [22] the use of Twitter posts to identify crimes by utilizing the BERT method (Bidirectional Encoder Representations from Transformers) to identify posts related to crime. Twitter posts are used to share environmental information. A paper authored by A. Muneer and S. M. F [23] proposes a technique for detecting cyberbullying on social media. This involves extracting tweets, applying text analysis methods that rely on predefined keywords to categorize the tweets, and then classifying them as either offensive or non-offensive. The outcomes of this evaluation could assist future researchers in selecting the right classifier for globally collected datasets of cyberbullying tweets. The paper [24] proposes a multi-task learning approach that uses Iterated Dilated Convolutional Neural Network (IDCNN) and Bidirectional Long Short-Term Memory (BiLSTM) machine learning algorithms to accurately detect cyber threat events on Twitter. The authors of the research [25] used Twitter data gathered from accounts connected to seven different places to conduct a case study in India. The study's objectives were to discover trends in tweets about crimes and examine the spatial distribution of crime in these areas. To evaluate the data and derive insights into crime trends in India, the authors used machine learning algorithms and natural language processing techniques. The authors of the paper [26] provided a method for locating tweets about crimes that need police intervention by analyzing Twitter data They used a text-mining approach to classify tweets into crime and non-crime classes. The authors M.Bs. and M. Azizi [27] proposed a hybrid method that combines deep learning and lexicon-based approaches, using BERT as the DL model, for categorizing and detecting crimes. The lexicon-based strategy and the BERT deep learning algorithm were used to classify and detect crimes. The authors Aine M, M. Moty, F. Iqbal B, et al. in the paper [28] proposed a method for identifying harmful content and "trolls" on social media platforms using deep learning techniques. The authors suggested that toxic images can be identified using machine learning based on the embedded text. The authors A. De, Sh. Kala and others proposed a model for detecting cyberbullying based on various features and implemented some of those features using a bidirectional deep learning model called BERT in their paper [29]. The authors of the paper [30] developed an automated classification model to recognize texts containing cyberbullying (CB) in a smart city using the Twitter engine. Sh. M. M. Matias and colleagues [31] created a model using machine learning to forecast cybercrime based on Twitter data. The authors Ne S, Sa Chandra, M K, et al [32], introduced two models, BCO-FSS and SSA-DBN, for detecting and classifying cyberbullying. They demonstrated through multiple simulations that their proposed FSSDL-CBDC method had better classification performance and highlighted the novelty of their study. The paper [33], presents a methodology for conducting a textual analysis of cyberbullying in the Arabic language using examples from social media platforms like Twitter, Facebook, and Instagram. The study aims to identify commonly used Arabic words or phrases that are used to harm others in a bias-free manner. The authors Firas S, Z. T, and E. introduced a novel framework in their paper [34] that uses Social Network Analysis (SNA) and Semi-Supervised Machine Learning (SSML) techniques to classify terrorist groups and user accounts. The framework samples online activities and behaviors to identify influential users. In this paper [35], the authors proposed a method that combines traditional lexical analysis with rapid text analysis and various feature extraction techniques to determine the intent of a text. The degree of intent detection is determined by analyzing the repetition of words and the victim's bully's degree of involvement. The proposed method aims to increase the computational efficiency of the model. The paper [36] by R. ALB and S. Abdallah presents the first Instagram Arabic corpus with a specific focus on cyberbullying sub-class categorization (multi-class). The dataset aims to identify offensive textual content. In their paper [37], BL. ABD, J ABA, and colleagues proposed a hybrid deep learning technique called DEA-RNN for detecting

cyberbullying on Twitter. The model combines an Elman-type Recurrent Neural Network (RNN) with a Dolphin Echolocation Algorithm (DEA) to optimize RNN parameters and shorten training time. By using this model, the authors aim to enhance the precision and efficiency of cyberbullying detection on social media platforms.

3. Social media's Effect on Cybercrime

Social media has a significant impact on cybercrime, including:

Social engineering assaults: Social media platforms make for the perfect setting for social engineering attacks by online criminals. Users can be duped into providing personal information or clicking on links that take them to phishing or malware download sites by using phony profiles [38].
Malware distribution: Via links and attachments, social media platforms can potentially be used to spread malware. Criminals online can set up phony accounts, publish links to harmful websites, or distribute malicious files that might infect users' devices. [39]
Identity theft: Personal data can be stolen from users of social media sites for identity theft. Cybercriminals can impersonate individuals or steal their identities to carry out fraudulent operations by using the information published on social media networks [40]
Cyberbullying: Even though the term "cyberbullying" did not even exist ten years ago, the issue is now widespread. Cyberbullies only require a cell phone or computer and the will to terrify; they do not need to be physically fit or quick. Anyone can engage in cyberbullying, and these individuals typically have few concerns about confronting their victims in person. Social media can be utilized for this type of bullying, which can cause psychological issues like emotional discomfort. Cybercriminals may utilize social media platforms to threaten or intimidate individuals or groups, which may harm those individuals' reputations as well as other consequences[[41]**.**
In general, social media has given cybercriminals new ways to launch assaults, but it has also given law enforcement and security experts new ways to track down and stop crimes. People should take precautions to protect themselves from online criminal activity.

4. Cybercrime Categories

There are many different kinds of cybercrimes, some of which include:`
Hacking: This is the act of breaking into a computer system, network, or website without authorization [42]
Malware: A malicious piece of software is one that is intended to damage computer systems or steal private information. Examples include Trojans, worms, viruses, and ransomware [43] [44] [45].
Phishing: This is the practice of tricking people into exposing private information, such as login credentials or financial information, by using phony emails or websites that look to be authentic [46]
Identity theft is the stealing of personal information with the intention of exploiting it fraudulently. This includes social security numbers, credit card numbers, and other identifying information.[47].

Cyberstalking: Using electronic communications to harass or threaten another person is known as cyberstalking [47]

Denial-of-service (DoS): DoS attacks include flooding a network or website with traffic in order to overwhelm it and render it inaccessible to users. To execute a DDOS assault through Facebook, the hacker develops malicious apps that include URLs related to the target's web server, which point to documents hosted by him [48]. As an intermediary, FacebookTM is being employed to carry out the attack in this situation. Despite the fact that Facebook users can monitor their profile material by configuring the appropriate privacy settings, thieves can still search for their personal information by using FacebookTM apps without their permission [49].

Cyberbullying is the use of electronic communication to harass or bully another individual [41]**.**
Online fraud refers to the use of the Internet to conduct fraudulent operations such as investment schemes, bogus online auctions, and other forms of deception [50]**.**
Cyber espionage is the theft of sensitive information from government agencies, corporations, or other organizations in order to achieve a political, economic, or military advantage [51]**.**
Child pornography refers to the production, distribution, or possession of sexually explicit images of children [52]. It's crucial to remember that cybercrime is an ever-changing field, with new sorts of assaults appearing all the time.

5. Comparison of cybercrime occurrences on social media platforms:

This part of the paper examines and evaluates the various studies discussed in section 2 to identify the common issues and challenges related to social media crimes. The authors focus on identifying the underlying causes of these issues. They present Table 1, which summarizes the key similarities and differences between the significant problems identified in the literature review

Table1. Important problems of the literature survey.

No. Ref	Problem
[18]	The study aimed is the automated detection of social media posts to prevent cyberbullying.
[19]	To overcome the difficulty of identifying the type of tweet due to the existence of an additional word in the keyword that matches all other words, The Aho-Corasick algorithm is used to identify the type of tweet based on the matching keyword.
[20]	A new system for detecting spam on Twitter is suitable for real-world applications.
[21]	The framework uses data from social media to anticipate cyberbullying, cyberstalking, online fraud, cyber harassment, and cyber hacking.
[22]	Using slang expressions, which were still understudied at the time this paper was being written, resolves the intention analysis of the post's problem.
[23]	The text analysis technique can be used to classify tweets and determine whether they constitute cyberbullying or not. Cyberbullying is a significant issue that affects both victims and communities.
[24]	To establish a highly accurate network model for problem-solving, Twitter's cyber threat events used a multi-task learning approach.
[25]	To address issues related to the analysis of real-time crime data using actual information gathered from security systems and social media datasets.
[26]	This statement suggests that identifying criminal messages in tweets can assist police in effectively utilizing patrolling resources.
[27]	It can almost solve complex problems as well as the human brain.
[28]	To address the issues of "trolling" and toxic behavior on social media platforms that are becoming more and more prevalent
[29]	A new method to detect hate speech on social media aims to tackle mental health issues caused by cyberbullying.
[30]	The paper presents a remedy to overcome the problem of overfitting that can affect the performance of the classifier, preventing it from generating a specific solution. The proposed approach involves Merging DNNs with the DT classifier to enhance the depth of the decision tree and recognize crucial tokens.
[31]	The issue with this paper Parts of speech or POS tags are not evaluated.
[32]	The use of deep learning models is proposed as a solution for detecting and categorizing cyberbullying on social media platforms to address this serious problem. This approach is considered essential for reversing the trend of cyberbullying.
[33]	Cyberbullying is a serious problem that is rapidly increasing and posing a concern for cybercrime investigators. Through social media platforms, cybercriminals can conduct various malicious activities such as data theft, tampering, distributed denial-of-service attacks, and cyberbullying.
[34]	The study aimed to identify Twitter accounts associated with terrorism using mining techniques and semantic analysis of tweets with a significant cyber-social impact.
[35]	The research paper discusses the difficulties children face as a result of digital media usage, including cyberbullying via fake accounts. To tackle this issue, the authors suggest employing artificial intelligence, natural language processing, and machine learning methods to automatically detect instances of online harassment.
[36]	With the use of a multi-class methodology, this work provides the first Arabic Instagram corpus for sub-class categorization to automatically identify the abusive language in Arabic social media content.
[37]	Primarily concentrating on the issue of Twitter's cyberbullying detection.

6. Comparisons of Crime Intelligence Tools Used in Social Media Crimes:

This section will compare several intelligence tools for detecting and predicting cyber crimes on social media and their drawback when used for detection or prediction, including NLP, machine learning, and deep learning, which we covered in Section 2 of this paper. In addition, the data set was used in papers that were collected for the literature survey. This section's goal is to examine the methods authors use to identify or predict criminal activity to gather data, as well as how they differ from literature surveys in terms of their drawbacks. Table 2, will present the most significant comparison.

Table2. Comparisons of Crime Intelligence Tools and drawback of literature survey

No. Ref	Intelligence tools	Drawback
[18]	The focus of this study was to compare the effectiveness of four machine learning algorithms in detecting instances of cyberbullying using two features - Bag-of-Words and term frequency-inverse text frequency. The four algorithms evaluated were Naive Bayes, Support Vector Machines, Decision Trees, and Random Forest.	Not specifying the data set is an obstacle when comparing research to other research.
[19]	The paper uses Aho Corasick, a ternary search, and a confusion matrix to assess experiment accuracy and prediction as well as KNN and SVM predictions at various phases.	The study lacks sufficient data to draw reliable conclusions.
[20]	The study evaluated nine supervised machine learning algorithms for classifying tweets as spam or non-spam. The algorithms were divided into five groups, and the study employed kNN, GBM, C5.0, NN, BLR, RF, NB, k-kNN, and DL to evaluate the performance of these algorithms.	Spammers use various techniques to avoid detection, to address this challenge the study employed parallel computing techniques to enable rapid updating of classification models.
[21]	This study uses a Multinomial Naive Bayes (MNB) and Support Vector Machine (SVM) model for tweet classification.	Using the official Twitter API without limiting the number of datasets
[22]	The pertained BERT for the Sequence Classification model is evaluated by comparing it with SVM, ANN+TF-IDF, and ANN+GloVe methods. BERT has a contextualized embedding layer, 12 configuration layers, and a classifier layer.	Research is ongoing to analyze the intention of posts containing slang expressions.
[23]	This study proposed a four-stage model for detecting cyberbullying, using TF-IDF and Word2Vec for feature extraction and noise reduction. The study employed seven machine learning classifiers to classify tweets as cyberbullying or non-cyberbullying, including Logistic Regression, Light Gradient Boosting Machine, Stochastic Gradient Descent, Random Forest, AdaBoost, Naive Bayes, and Support Vector Machine.	The paper did not extensively investigate feature extraction methods, which were limited to only two methods, in comparison to the use of seven machine learning classifiers.
[24]	Multi-task learning combines machine learning algorithms with natural language processing techniques to create a precise network model and named entity extraction. The approach involves creating a precise network model using IDCNN and BiLSTM, followed by named entity extraction using Stanford Core NLP.	- Tweet compilation took a long time
[25]	The study used sentiment analysis to track the criminal activity on Twitter. By analyzing a large collection of unlabeled tweets using Brown clustering which provided better performance than traditional models in predicting crime rates.	Advanced filtering tools can improve accuracy performance.
[26]	The study used classifiers such as Naive Bayesian, Random Forest, J48, and ZeroR, for text mining-based classification. and data pre-processing techniques to improve classification accuracy.	Drawback Action Lack of crime tweet location information that assists police in locating a crime.

[27]	The study used a lexicon-based approach and a BERT model for sentiment analysis on a Twitter dataset. The BERT model was implemented with special tokens, attention masks, and padding, and the softmax function was used for prediction.	The limitations of sentiment analysis in dealing with metaphorical, sarcastic, and encrypted expressions in English are highlighted in this statement. Computational models and methods still struggle to handle complex sentences.
[28]	The study proposes a text classification and image text extraction module to extract text from images and use it to test a deep learning model based on bidirectional LSTM and bidirectional GRU recurrent neural networks for toxicity detection.	Regular networks and two-way networks differ in classification, but not significantly.
[29]	The study suggests a sentiment analysis model categorizes subjective information into five groups for cyberbullying detection. The model combines three BERT model embedding to handle sequential data.	Using the official Twitter API without limiting the number of datasets.
[30]	The study proposed The Deep DT approach for classifying cyberbullying tweets which includes techniques such as tokenization, lemmatization, and text feature extraction using Information Gain, Chi-Square 2, and Pearson Correlation. The study finds that DNN predictions are more accurate than ANN networks and uses Rectified Linear Units to avoid overfitting.	- Implement three distinct methods for feature extraction to lessen the issue of noisy data
[31]	With a focus on preprocessing and sentiment analysis, Researchers studied cyberbullying and cyber threats using Naive Bayes, Decision Tree, and Support Vector Machine algorithms.	The study cannot detect emojis, which may be an important aspect of interpreting people's sentiments.
[32]	The BCO-FSS method and SSA-DBN model are used to detect and categorize cyberbullying in online settings. The SSA algorithm and BCO algorithm are used to detect and characterize cyberbullying. while the BCO algorithm selects features to improve classification performance.	No drawback
[33]	A Decision Tree (DT) algorithm is used to train the system model to identify cyberbullying in the Arabic language.	The study uses the Twitter API to obtain a larger and more diverse set of data to be used in the analysis.
[34]	The study used BERT to identify extremist Twitter accounts and SVM, Naive Bayes, and Logistic Regression classifiers to identify influential members. The paper used feature selection algorithms to identify influential members of extremist communities. Algorithms used to counter online extremism include Bag of Words, Part of Speech tags, and TF-IDF.	The studies highlight some drawbacks of using feature selection algorithms like Bag of Words, Part of Speech tags, and others for text mining to identify extremist Twitter profiles. The use of co-occurrences, bi- and trigrams, and N-grams can reduce the accuracy of text mining.
[35]	The study uses fast text and POS tagging can be used to identify harassing comments but can lead to poor performance when dealing with imbalanced datasets.	Ensemble-based deep learning can reduce bias and variation in machine learning models.
[36]	Preprocessing techniques, TF-IDF, and classical classifiers are used to analyze Instagram harassment.	The diversity of dialects in Arabic presents a challenge for cyberbullying classification.

[37]	The DEA-RNN model combines Dolphin Echolocation Algorithm and Elman-type Recurrent Neural Networks to identify cyberbullying. The model was evaluated using 10,000 tweets and compared to other algorithms. SMOTE is used to oversample the minority class to address the class imbalance.	Only the content of tweets was examined; user behavior was not taken into account.

7. Discussing the Results of A study and its Future Work:

This section addresses the limitations of using automated methods for crime detection and explores the potential of social media as a tool for detecting criminal activities. While social media can provide valuable insights for law enforcement, criminals can modify their behavior to evade detection, making it challenging to apply detection techniques across different domains. Nonetheless, there could be some similarities between crimes committed in the physical world and those committed on social media. Table 3 summarizes the findings of the literature review, dataset, and future work.

Table 3. A Comparison between The results, Data set, and Proposed Future Work.

Ref	Data set	The Results	The future work
[18]	Perform experiments using two sets of comments and posts from Facebook and Twitter.	The study found that SVM was the top-performing machine learning algorithm, with TF-IDF performing better than BoW.	The future work will involve Deep learning algorithms will be used to detect and categorize cyberbullying in Bengali language texts.
[19]	The study collected data from Twitter using the Twitter 4j API from two datasets, which consisted of 1000 tweets and 250 tweets.	The study assessed the performance of KNN and SVM algorithms that predicted lower percentages of severe terrorist attacks than actual data. KNN predicted 26.76%, SVM 29.79%. The study analyzed 250 datasets and found 30% of severe terrorist attacks.	The proposed approach involves adjusting keyword selection and pattern analysis to predict and prevent terrorist attacks, using machine learning to identify COVID-19-affected areas.
[20]	The study used 6.5 million tweets to test the effectiveness of parallel computing.	Deep Learning outperformed other algorithms in accuracy, TPR, FPR, and F-measure. Random Forest and C5.0 outperformed the other methods in terms of detection accuracy, TPR, FPR, and F-measure. Deep Learning achieved 80% and over 80% TPR and F-measure accuracy with 200k training data.	Future research can improve tweet collection methods and spam detection can enhance the prototype system for near real-time Twitter spam detection.
[21]	- The dataset was retrieved using the official Twitter API.	An ANN-based categorization technique achieved an accuracy rate and AUC of 92.8% and 0.982, respectively. The neural network model had an average loss function of 0.195 and 0.220, and an average accuracy of 0.926 and 0.942, respectively. Additionally, the suggested BERT model had an AUC of 0.984.	-
[22]	More than 100,000 tweets were collected between January 1 and January 31, 2020.	Logistic regression was the most accurate classifier which had a median accuracy of almost 90.57%. with SGD having the highest precision, SVM having the highest recall, and LR having the highest F1 score. Multinomial	Future research, according to the author, should concentrate on identifying cyberbullying in

	(Assault, Burglary, Drunk Driving, Homicide, Sex Crimes, Suicide)	NB and Multinomial RF showed low detection rates (81.39%) and execution times (0.014s and 2.5287s, respectively) but also low accuracy and precision.	different languages, particularly in an Arabic environment.
[23]	The dataset consists of 37,373 tweets, 30% of which are used for prediction and 70% for training.	The model achieved an F1-score rate of 96.4% using 5-fold cross-validation IDCNN with BiLSTM and CRF performed better than other entity recognition techniques in the NER task.	Future research will improve the efficiency and accuracy of extracting cyber threat events from tweets.
[24]	Network security-related datasets were gathered for model training.	The study analyzed crime rates in seven Indian cities using social media and found a detection accuracy of approximately 70%. The study found that Ghaziabad had the highest crime intensity, while Jammu had the lowest. The study found that identifying cities with high and low crime rates was the most important result.	In the future, next-generation language processing, deep learning, and machine learning will be used to increase the precision of the findings. Additionally, using more sophisticated and intelligent filtering tools could improve the research's accuracy performance.
[25]	Using Twitter's API, the dataset contains 11,073 tweets about cybersecurity over a year, from January 1 to June 1, 2020, including tweets about "DDOS," "ransomware," "data breach," "phishing," and other topics	The study evaluated four classifiers using accuracy, precision, recall, and F1 score on a sizable dataset and found that Random Forest had the highest accuracy rate of 98.1%, while ZeroR had the lowest accuracy rate of 61.5%. The study also used ROC analysis to address imbalanced datasets and found that classifier selection is crucial for accurate predictions in such datasets.	The research will need to be expanded by using Classifiers, location information, ensemble learning-based approaches, and NLP techniques, and the proposed approach needed to expand research and proposed approach will need to be compared to other approaches.
[26]	The study collected Twitter data from seven Indian cities from January 2014 to November 2018. to validate crime statistics from 2014-2016.	The proposed strategy for identifying crimes on Twitter achieved an F1-score of 94.92, a classification accuracy of 94.91%, a loss of 16.26%, a precision of 94.94%, and a recall accuracy of 93.91%. The proposed strategy could be a useful tool for identifying criminal activity on social media platforms. Based on the outcomes, the precision, recall, and F-measure scores of the three algorithms are all higher than 0.9.	Using other algorithms to develop the proposed work in the future
[27]	Twitter collected 500 tweets in its real-time dataset. 230 (non-crime) or 270 (crime)	Based on the outcomes, the precision, recall, and F-measure scores of the three algorithms are all higher than 0.9.	--
[28]	The study analyzed 70,000 tweets, including 27,000 tweets related to crimes and 43,000 regular tweets.	The study assessed three classifiers' effectiveness in detecting toxic comments, highlighting the importance of improving text extraction from images and using standard fonts. Achieved an F1-score and testing accuracy of 0.92.GloVe word embedding improved models' accuracy in extracting and categorizing text from online messages.	--

	divided into 18,000 crime-related and 37,000 regular tweets, using Twitter's streaming API.		
[29]	The Conversation AI team produced the dataset to participate in a Kaggle NLP challenge (Jigsaw, 2022). The dataset has six labels: identity hate, obscene, threat, toxic, and severely toxic.	The BERT model outperformed conventional machine learning models in assessing sentiment in text documents. with a high accuracy rate of 91.90%.The model demonstrated better accuracy on Twitter than SVM (52.70%) and Naive Bayes (71.25%) models.	Future research will focus on creating a model to accurately recognize cyberbullying and differentiate it from non-bullying texts. The goal is to improve the model's ability to recognize cyberbullying.
[30]	The official Twitter API is used to extract the dataset.	A suggested classifier's performance is evaluated using various measures, such as precision, sensitivity, specificity, accuracy, F-measure, and G-mean, and compared to currently used machine learning classifiers. The Deep DT classifier achieved the highest classification accuracy when trained using the Pearson correlation feature selection method. Using the Pearson Correlation feature selection method improves classification accuracy. The suggested technique outperforms current classifiers in accuracy when using 90% of training data	The paper suggests further research into Researchers should test a hybrid strategy combining deep learning and optimization to handle high-dimensional datasets in practical applications. To enhance the effectiveness of this approach, the authors suggest testing it on real datasets.
[31]	30,384 tweets were utilized, comprising both CB and non-CB tweets that had not been manually tagged or labeled.	The model was trained on 75% of the data and tested on the remaining 25%, The Naive Bayes algorithm achieved 86%, the Decision Tree algorithm 91%, the Logistic Regression algorithm 93%, and the Random Forest algorithm 93%.	Future research could take a different course as a result of model comparison and the application of a neural network.

[32]	The dataset was created in real-time by using the official Twitter API. 100 tweets about the specified search query will be gathered by the process.	The SSA-DBN model outperforms other algorithms with a 99.983% higher accuracy. The FSSDL-CBDC technique is shown to be superior to other methods in various ways based on experimental results.	To increase performance, FSSDL-CBDC combines outlier identification and feature reduction for real-time analysis of high-dimensional data. Feature selection (FS) is used for outlier identification in streaming data for network security and intrusion detection.
[33]	Traditionally, the study is conducted using an available dataset.	The model achieved a 99.08% accuracy rate and identified instances of cyberbullying on Twitter, Facebook, and Instagram with a detection rate of 81.12%. The model was evaluated using F1-score and Random Forest classifiers, with the Random Forest classifier achieving 70% in training and 50% in testing, and the F1-score classifier achieving 56.05% in training and 74% in testing.	Future iterations of this work will investigate machine learning and deep learning algorithms to recognize offenses connected to cyberbullying utilizing a variety of data forms, including audio, video, and photographs.
[34]	'API libraries' were utilized for the data collection process.	The results of the study are evaluated using standard classification metrics, and the framework proposed in the study is effective in combating Twitter extremism, outperforming other approaches.	-
[35]	-The obtained dataset, which contains about 50,000 Words, served as the algorithm's training data.	The model outperforms current classification techniques in accuracy and error rate and adds fast text to reduce time complexity. The model outperforms J48, NB, SVM, RF, bi-LSTM, and MLP neural networks.	The performance of the model can be enhanced by integrating different machine learning classifiers.
[36]	- 'API libraries' were used for data collection.	The SVM classifier is the best choice for bullying remarks and performs the best with an F1 score of 69%outperforming the other classifiers due to its near-perfect agreement among annotators. The RFC classifier has a 67% F1 score for bullying comments, with Positive remarks having the most useful metrics. The p-value of 0.869 shows near-perfect agreement among annotators, making the SVM classifier the best choice for this issue.	-.
[37]	The dataset included 155,260 Instagram posts with an average word count of 12 and 8203 non-harassments and 2754 harassment-related comments. The dataset is unbalanced, with 75% non-harassment comments and 25% harassment comments.	By extensive experimental findings using several metrics like recall, precision, accuracy, F1-score, and specificity, the proposed DEA-RNN model is shown to be superior to three machine learning models (SVM, MNB, and R), two deep learning models (Bi-LSTM and RNN), and one model (RNN). Using Twitter datasets, DEA-RNN is tested using several scenarios, with scenario 3 outperforming other models in terms of accuracy, precision, recall, F1-score, and specificity (90.94%, 89.95%, 88.98%, and 89.25%).	-

8. Preventive Procedures And Protection Mechanisms For Cyber Crimes In Social Media

Technology advances can be utilized to manage, deter, protect, and prosecute crime in the same way that criminals use social media to commit crimes. Law enforcement agencies can utilize comparable platforms to file charges against offenders. Criminals might use social networking sites to discover possible targets [53]. For instance, Toronto police frequently use social media to find the most sought criminals in the city [17]. All social media users, whether people or corporations are advised to exercise caution when disclosing personal information that could be used against them by criminals, according to a proposal made by Duncan Smeed, George R. S. Weir, and Fergus Tool [54]. Security precautions must be taken. Some strategies for preventing cybercrimes include updating all software, knowing your friends well, using up-to-date antivirus software, learning the fundamentals of security, avoiding sharing sensitive information, and using strong passwords [55] In order to avoid attacks and effectively respond to them, networks commonly use network policy management tools like antivirus, firewall, anti-malware, perfusion framework spam filter, intrusion, and anti-virus software. The author also discusses security managers, security concerns, and networks that use these tools. It's crucial to find solutions for security issues and a strategy for shielding data from social media attacks.

9. Dataset Availability:

During our review of the research to conduct a survey that includes cyber crimes on social media, the authors that provided the data set availability are shown in Table 4, and according to the order of the search site within the reference.

Table 4. Dataset Availability

No. Ref	Dataset Availability link
18	https://www.kaggle.com/datasets
23	https://github.com/das-lab/Cyberthreat-Detection
24	http://www.cs.cmu.edu/~ark/TweetNLP/
28	https://www.kaggle.com/competitions/jigsaw-multilingual-toxic-comment-classification/data
36	https://bit.ly/3Md8mj3

10. Conclusion

Social media platforms are used for shady activities like terrorist recruitment, fraud, cyberbullying, and hacking. Social media companies must monitor their platforms and ban users who break the law while weighing the right to free speech against steps to stop malicious intent. Dissemination of information, account profiling, and content analysis are strategies for locating different kinds of crimes. We looked at cybercrime across social media platforms Twitter, Facebook, and Instagram, using a variety of crimes, including terrorism, cyberbullying, or phishing, as well as crime analysis, including the Twitter platform. The authors were reviewed for the period (2020-2022). When we reviewed research related to the field of crime detection via social media for the totality of the literature survey and different types, although we were able to monitor the effectiveness and security of the algorithms used in all types of machine learning and NLP In addition to deep learning, social media can be used as a tool to facilitate various types of crimes such as cyberbullying, identity theft, fraud, and harassment, Accurately estimating the **percentage of crimes** committed by social media during the research review phase for the aforementioned years may be insufficient because the research we conducted does not represent all research on all international sites. We are studying a sample of these crimes and the reason for the increase in crimes as a result of the misuse of social media, as they are used by individuals who do not have sufficient experience or individuals with experience in this field and exploit them to achieve crime. Therefore, both individuals and organizations must take precautions against electronic crimes and raise awareness of the dangers of using social media. Additionally, to prevent cybercrime and protect people from harm, law enforcement organizations and social media platforms need to collaborate. In this paper's review of the literature survey, the methods proposed by the researchers were also briefly discussed and examined and their effectiveness was compared. This study will be a tool for creating new technologies, updating existing technologies, and enhancing safety by anticipating and detecting crimes. The paper also proposes sharing detection models through a central repository to enable assignment to new domains. Crime detection and reduction.

Acknowledgments

The authors would like to thank 1Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics (https://iips.edu.iq/), Baghdad-Iraq for its support in the present work.

REFERENCES

[1] Bal Krishna Shah, Nitu Sharma, Saloni Bandgar and Prof. Sainath Patil, "Cybercrime Prevention on Social Media," *International Journal of Engineering Research & Technology (IJERT),* Vols. Vol. 10 ,NO 03, March, no. ISSN: 2278-0181,, 2021.

[2] Brett Drury c d, Samuel Morais Drury e, Md Arafatur Rahman f, Ihsan Ullah, "A social network of crime: A review of the use of social networks for crime and the detection of crime"," *Online Social Networks and Media,* vol. Volume 30, July 2022.

[3] Jolan Rokan Naif1, Ghassan H. Abdul-majeed2, Alaa K. Farhan[3], "Internet of Things Security using New Chaotic System and Lightweight AES," *AL-Qadisiyah for computer science and mathematics,* vol. Vol.11,. No.2, 2019.

[4] Z. Abbass, Z. Ali, M. Ali, B. Akbar, and A. Saleem, "A Framework to Predict Social Crime through Twitter Tweets By Using Machine Learning," *IEEE 14th International Conference on Semantic Computing (ICSC),* pp. 363-368, 2020.

[5] J. Pereira-Kohatsu, L. Quijano-Sánchez, F. Liberatore and Camacho-Collados, "Detecting and Monitoring Hate Speech in Twitter," *Sensors,* 19-2019.

[6] Yagcioglu, S.; Seyfioglu, M.S.; Citamak, B.; Bardak, B.; Guldamlasioglu, S.; Yuksel, A.; Tatli, E.I," "Detecting Cybersecurity Events from Noisy Short Text," *North American Chapter of the Association for Computational Linguistics (NAACL),* p. 1366–1372, 2019.

[7] Mazoyer, B.; Cagé, J.; Hervé, N.; Hudelot, C, "A French Corpus for Event Detection on Twitter," *Proceedings of the 12th Language Resources and Evaluation Conference, Marseille, France,* p. 6220–6227, 11–16 May 2020.

[8] I. Idrissi, M. Boukabous, M. Azizi, O. Moussaoui, and H. El Fadili "Toward a deep learning-based intrusion detection system for IoT against botnet attacks," *IAES International Journal of Artificial Intelligence (IJ-AI),* vol. vol. 10, no. 1, pp. 110-120,, Mar. 2021.

[9] M. B. a. M. Azizi, "Augmented binary multi-labeled CNN for practical facial attribute classification," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. vol. 23, no. no. 2, pp. 973-979, 2021.

[10] R. A. K. N. V. S. T. E. Z. a. S. S. Z. E. A. Kirillova, "Problems of fighting crimes on the internet," *Journal of Advanced Research in Law and Economics,* vol. vol. 8, no. no. 3, p. pp 849–856, Jun. 2017.

[11] D. N. H. A. K. F. Rusul Mansoor Al-Amri1, "Generation Initial Key of the AES Algorithm based on Randomized and Chaotic System," *Al-Salam Journal for Engineering and T technology,* vol. vol. 2 , no. No. 1 , pp. p p. 53-68,, 2023.

[12] A. S. C. M. H. B. T. J. B. N. a. M. P. A. Agarwal, "Identification and Classification of Cyberbullying Posts: A Recurrent Neural Network Approach Using Under-Sampling and Class Weighting," *Neural Information Processing (Communications in Computer and Information Science,* vol. vol. 1333, no. H. Yang, K. Pasupa, A. C.-S. Leung, J. T. Kwok, J. H. Chan, and I. King, Eds. Cham, Switzerland: Springer, p. pp. 113_120, 2020.

[13] S. Alhassun 1, and Murad A. Rassam , "A Combined Text-Based and Metadata-Based Deep-Learning Framework for the Detection of Spam Accounts on the Social Media Platform Twitter," Processes-MDP, vol. 10, no. 3, pp. 1-24, 22 February 2022.

[14] B. A. H. Murshed, H. D. E. Alkriki, and S. Mallappa, " Semantic analysis techniques using Twitter datasets on big data: Comparative analysis study," *Comput. Syst. Sci. Eng.,* vol. 35, no. 6, p. 495_512, 2020.

[15] Safa S. Abdul-Jabbar1 and Alaa K. Farhan, "Data Analytics and Techniques: A Review," *ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY,* Vols. 10 no. 2 , 2022.

[16] R. Sawyer, "The Impact of New Social Media on Intercultural Adaptation," University of Rhode Island, 5-2011.

[17] Lama Almadhoor, bFaiz Alserhani, cMamoona Humayun, "Social Media and Cybercrimes,," *Turkish Journal of Computer and Mathematics Education,* vol. 12, no. 10, pp. 2972-2981, 2021.

[18] Md Manowarul Islam; Md Ashraf Uddin; Linta Islam; Arnisha Akter; Selina Sharmin; Uzzal Kumar Acharjee, "Cyberbullying Detection on Social Networks Using Machine Learning Approaches," in *IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE),* Asia-Pacific, 2020.

[19] Aditi Sarker, Partha Chakraborty, S. M. Shaheen Sha, Mahmuda Khatun, Md. Rakib Hasan, Kawshik Banerjee, "Improvised Technique for Analyzing Data and Detecting Terrorist Attack Using Machine Learning Approach Based on Twitter Data," *Journal of Computer and Communications* , vol. 8 , no. 7, July 30, 2020.

[20] Sun, Nan; Lin, Guanjun; Qiu, Junyang; Rimba, Paul, "Near real-time Twitter spam detection with machine learning techniques," *International Journal of Computers and Applications,* vol. 44, no. 4, pp. 338-348, 2020.

[21] Sreya C M ,"A Framework To Predict Social Crimes Using Twitter Tweets," *(IJRASET) International Journal for Research in Applied Science & Engineering Technology,* vol. 9, no. 1, Jan 2021.

[22] S.P.C.W Sandagiri; B.T.G.S Kumara; Banujan Kuhaneswaran, " Deep Neural Network-Based Approach to Identify the Crime-Related Twitter Posts," in *International Conference on Decision Aid Sciences,* 2020.

[23] Muneer, Amgad; Fati, Suliman Mohamed, " A Comparative Analysis of Machine Learning Techniques for Cyberbullying Detection on Twitter

12(11), 187–. doi:10.3390/fi12110187," *Future Internet*, vol. 12, no. 11, 2020.

[24] Fang, Yong; Gao, Jian; Liu, Zhonglin; Huang, "Detecting Cyber Threat Events from Twitter Using IDCNN and BiLSTM," *Applied Sciences*, vol. 10, no. 17, p. 5922, 2020).

[25] Vo, Thanh; Sharma, Rohit; Kumar, Raghvendra; Son, Le Hoang; Pham, Binh Thai; Tien Bui, Dieu; Priyadarshini, Ishaani; Sarkar, Manash; Le,, "Crime rate detection using social media of different crime locations and Twitter part-of-speech tagger with Brown clustering," *Journal of Intelligent & Fuzzy Systems*, vol. 1, no. 13, 2020.

[26] Vijendra Singh, Vijayan K Asari, Kuan-Ching Li, "Analysis and Classification of Crime Tweets," *Procedia Computer Science*, vol. 167, pp. 1-2662, 2020.

[27] Mohammed Boukabous, Mostafa Azizi, "Crime prediction using a hybrid sentiment analysis approach based on the bidirectional encoder representations from transformers," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 2, pp. 1131~1139 ISSN: 2502-4752, February 2022, .

[28] Aine MacDermott a, *, Michal Motylinski a, Farkhund Iqbal b, Kellyann Stamp a, Mohammed Hussain b, Andrew Marrington, " Using deep learning to detect social media 'trolls," *Forensic Science International Digital Investigation*, vol. 43, no. 1, p. 301446, September 2022.

[29] Aditya Desai1, Shashank Kalaskar2, Omkar Kumbhar3, and Rashmi Dhumal4, " Cyberbullying Detection on Social Networks Using Machine Learning Approaches," in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Gold Coast, Australia, 16-18 December 2020 .

[30] Natarajan Yuvaraj; Victor Chang; Balasubramanian Gobinathan; Arulprakash Pinagapani; Srihari Kannan; Gaurav Dhiman; Arsath Raja Rajan, "Automatic detection of cyberbullying using multi-feature-based artificial intelligence with deep decision tree classification," *Computers & Electrical Engineering*, vol. 92, p. 107186, June 2021.

[31] Sheila Marie M. Matias; Jefferson A. Costales; Christian M. De Los Santos, "A Framework for Cybercrime Prediction on Twitter Tweets Using Text-Based Machine Learning Algorithm," in *2022 5th International Conference on Pattern Recognition and Artificial Intelligence (PRAI)*, Chengdu, China, 19-21 August 2022.

[32] Neelakandan S.[1] Sridevi M,[2] Saravanan Chandrasekaran,[3] Murugeswari K,[4] Aditya Kumar Singh Pundir ,[5] Sridevi R,6 and T.Bheema Lingaiah, "Deep Learning Approaches for Cyberbullying Detection and Classification on Social Media," *Computational Intelligence and Neuroscience*, vol. 2022, p.1- 13,11 June 2022.

[33] Ohoud Alshabiba, Dr.Faeiz Mohammed Al Serhanib, and Dr.Randa Ahmed Jabeurc, " Investigation Cyberbullying Crime in Social Media Application," *Turkish Journal of Computer and Mathematics Education* , vol. 13, no. 3, pp. 317-323, 2022.

[34] Firas Saidi a, Zouheir Trabelsi b, Eswari Thangaraj b, " A novel framework for semantic classification of cyber-terrorist communities on Twitter," *Engineering Applications of Artificial Intelligence*, vol. 115, p. 105271, October 2022.

[35] S. Abarna a,*, J.I. Sheeba a, S. Jayasrilakshmi a, S. Pradeep Devaneyan b, " Identification of cyber harassment and intention of target users on social media platforms," *Engineering Applications of Artificial Intelligence*, vol. 115, p. 105283, (2022.

[36] Reem ALBayari and Sherief Abdallah, " Instagram-Based Benchmark Dataset for Cyberbullying Detection in Arabic Text," *Licensee MDPI*, vol. 7, no. 83, 2022.

[37] Belal Abdullah Hezam Murshed[1-2], Jemal Abawajy [3], (Senior Member, IEEE), Suresha Mallappa[1], Mufeed Ahmed Naji Saif [4], and Hasib Daowd Esmall ALariki[5-6], "DEA-RNN: A Hybrid Deep Learning Approach for Cyberbullying Detection in Twitter Social Media Platform," in *IEEE Access (Volume: 10)*, 23 February 2022.

[38] Zainab Alkhalil, Chaminda Hewage *, Liqaa Nawaf and Imtiaz Khan, " Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science*, vol. 3, 09 March 2021.

[39] Z. Zulkefli, M. M. Singh, A. R. M. Shariff, and A. J. P. C. S. Samsudin, "Typosquat Cyber Crime Attack Detection via Smartphone,"," *Procedia Computer Science*, Vols. 124, pp. 664-671, 26 December 2017,.

[40] Nicole Leeper Piqueroa, Alex R. Piqueroa,b, Stephen Giesc, Brandn Greenc, Amanda Bobnisc, and Eva Velasquez, " Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders," *VICTIMS & OFFENDERS*, vol. 16, no. 3, p. 444–463, 2021.

[41] S Charles E. Notar*, Sharon Padgett, Jessica Roden, Cyberbullying, " Cyberbullying: A Review of the Literature," *Horizon Research, Universal Journal of Educational Research*, vol. 1, pp. 1-9, 2013.

[42] Alferidah, Dhuha Khalid, and N. Z. Jhanjhi. "A Review on Security and Privacy Issues and Challenges in Internet of Things, " A Review on Security and Privacy Issues and Challenges in Internet of Things," *International Journal of Computer Science and Network Security IJCSNS*, vol. 20, no. 4, pp. 263-286, 2020.

[43] Ubing, A. A., Jasmi, S. K. B., Abdullah, A., Jhanjhi, N. Z., & Subramaniam, M., "Phishing website detection: An improved accuracy through feature selection and ensemble learning," *(IJACSA) International Journal of Advanced Computer Science and Applications*,, vol. 10, no. 1, pp. 252-257, 2019.

[44] M. Omar Saeed Al, "Threats and Anti-threats Strategies for Social Networking Websites," *International Journal of Computer Networks & Communications*, vol. 5, pp. 53-61, 2013.

[45] M. R. Faghani, A. Matrawy, and C. H. Lung, "A Study of Trojan Propagation in Online Social Networks," in *5th International Conference on New Technologies*, 2012.

[46] M. Dadkhah, M. Lagzian and G. Borchardt, "Identity Theft in the Academic World Leads to Junk," *Science and Engineering Ethics,*, vol. 24, no. 1, p. 287–290, 2018.

[47] K. P. e. a. DM Chudasama, "Awareness of Data Privacy Breach in Society," *International Journal of All Research Education and Scientific Methods (IJARESM)*, vol. 8, no. 10, pp. 303-307, 2020.

[48] A. Cleeff, R. Wieringa, v. P. Eck, and V. N. L. Franqueira, "A. Cleeff, R. WiEngineering security agreements against external insider threat," *Information resources management journal,*, vol. 26, pp. 66-91, 2013.

[49] Alferidah, Dhuha Khalid, and N. Z. Jhanjhi, "A Review on Security and Privacy Issues and Challenges in Internet of Things," *International Journal of Computer Science and Network Security IJCSNS*, vol. 20, no. 4, pp. 263-286., 2020.

[50] . J. Clement, "Most popular social networks worldwide as of July 2020," *ranked by the number of active users(in millions)*, 29 Oct 2020.

[51] Niraja K.S., Srinivasa Rao S, "A hybrid algorithm design for near real-time detection cyber attacks from compromised devices to enhance IoT security Mater," *Today: Proc*, 5 March 2021.

[52] Ethel Quayle, "Self-produced images, sexting, coercion, and children's rights," *ERA Forum*, vol. 23, p. 237–251, 2022.

[53] R. D'Amore, "Toronto police tap into power of social media to catch city's most wanted criminals," *CTV News Toronto*, 2018 Updated November 12, 2020.

[54] Parlakkılıç, Alaattin, " Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach.," *International Journal of Information Security Science*, vol. 7, no. 4, pp. 172-178., 2018.

[55] Khan, N. A., Brohi, S. N., & Zaman, N, " Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.," *TechRxiv Powered by IEEE - 2020*, 2020.

[56] Weulen Kranenbarg M, Ruiter S, van Gelder JL, Bernasco W, " Cyber-Offending and Traditional Offending over the Life-Course: an Empirical Comparison," *J Dev Life Course Criminol.* , vol. 4, no. 3, pp. 343- 364, 2018.