

An Approach to Profiler Detection of Cyber Attacks using Case-based Reasoning

Marc Krüger^{1,2,*,†}

¹ Institute of Computer Science, Intelligent Information Systems, University of Hildesheim, Hildesheim, Germany

Abstract

Cyber attacks not only have an enormous economic damage potential for companies and authorities, but also represent a high risk in the area of critical infrastructures. It is therefore necessary to develop new procedures that enable the profiling of cyber attacks, also with regard to constantly growing amounts of data. This leads to the question of how artificial intelligence can be used as a tool in the field of cybercrime to find solutions to current challenges. Based on these findings, an application system in the field of case-based reasoning, which is a subfield of AI, is presented. Insights into the various subfields of computer science, such as speech recognition, malware analysis or recognition of text duplicates, are made possible.

Keywords

Cybercrime, Case-based reasoning, Profiling, Artificial Intelligence

1. Introduction

According to a report by the World Economic Forum, cybercrime will be the second biggest risk for companies in the next ten years [1]. Rising numbers of reported cybercrime offences and now diverse modi operandi show that it is relevant for both companies and private individuals to protect themselves. In the course of this, it is of importance to identify current challenges in this research area in order to counteract them with developed solution approaches. Accordingly, recent research shows which steps are to be taken in the environment and challenges of cybercrime. For example, the World Economic Forum points out in its 2020 publication "First Steps" that increasing cyber resilience will better protect potential victims [2]. The formation of public-private cooperation, for example between authorities and associations in the cybercrime environment, leads to mutual benefit. Another publication of the World Economic Forum, "Take action on Cybercrime", also points out the absolute necessity of collaborative action through the establishment and development of joint global architectures against cybercrime. The number of cyber attacks rose to around 87,106 cases in 2018 [3]. Around 22,000 suspects were identified during investigations. At the same time, with the introduction of 5G and the further dovetailing of everyday habits with the digital world, the volume of data is increasing immensely. Manual evaluation is more difficult from this point of view, so that automated profiling of cyber attacks is called for in the face of rapidly increasing data volumes. It is true that search engines can also be used here to obtain corresponding characteristics of a cyber attack. The problem here is

LWDA'22: Lernen, Wissen, Daten, Analysen. October 05–07, 2022, Hildesheim, Germany

✉ krueger.hannover@t-online.de (M. Krüger)



© 2022 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

that if the formulation is too soft, the investigator will be provided with too large a selection of data records. Accordingly, if the formulation is too sharp, the result set will be too small or will not return any value at all. Likewise, the search engines do not fall back on previous search queries with the delivered results. In this case, stored knowledge can be very valuable for determining the results. The search engine could thus make use of experience values and return well-established results based on experience.

Due to the large amount of data, artificial intelligence is increasingly being used in the field of law enforcement [4]. One approach in the field of AI to problem solving is to use old case experiences to solve a current problem situation [5]. Case-based reasoning software systems are knowledge-based systems and process tasks on the basis of known solutions for similar problems by comparing the "new" problem with already stored cases. The system offers the user similar cases that can either be adopted, adapted or discarded. A case-based reasoning approach is used, in which all cases that have occurred are stored in a case database. If certain parameters are entered for a current problem situation, a CBR system searches for cases with similar parameter values ("experiences") from the case base and offers them as possible solutions. A user decides whether a solution is adopted, modified or completely new. The solution thus determined is added to the case base. In the area of cybercrime cases, a case-based reasoning system lends itself to this, since the "knowledge" is stored in a case base. In most existing systems, there should already be an existing case base, so that when a CBR system is used, it can access it. The CBR cycle according to Aamodt and Plaza consists of the steps 'Retrieve', 'Reuse', 'Revise' and 'Retain' [6]. In the retrieve stage, the system first selects suitable cases from the case base on the basis of a query. In the Reuse phase, a subsequent analysis leads to the creation of a solution proposal for the new case. In the third stage, Revise, proposed cases are evaluated. If the proposed solution is accepted, the current case is saved in the case base in the retain phase. Each case thus represents a problem and the corresponding solution in the knowledge base.

Case-based reasoning uses existing stored knowledge to derive suggested solutions. The research paper is structured as follows: chapter 2 reviews the relevant literature, chapter 3 explains the methodology used in the research, and chapter 4 presents the research hypotheses and the corresponding results. Finally, chapter 5 summarises these findings and suggests further research and future work.

2. Related work

Cyber attackers cause great damage and can thus be classified as serious crimes. The chapter shows work on profiling cyber attacks and conceivable identification of the human criminals behind them. In 1984, Steven Levy coined the definition of hacker ethics [7]. Further subdivisions followed in Landreth 1985 into novice, student, tourist, crasher and thief [8]. Hollinger categorised in 1988 into pirates, browsers and crackers [9]. Rogers differentiated in 2000 into newbie, cyberpunks, internal, coders, old-guard-hackers, professional criminals and cyberterrorists [10]. In particular, the motivations and characteristics of the respective perpetrators were recorded. Questionnaires were also used in the hacker profiling project to record attributes such as age or gender and the reasons for the behaviour. These studies on cyber attackers were very socio-ethnically oriented and allow profiling on the respective person with their personal environment. However, such studies do not allow for technical mechanisms to record the characteristics of a cyber attack in an IT-based manner. Defence measures therefore focus on the characteristics of cyber attacks. For example, cyberattacks carried out by botnets are recorded according to similarity characteristics such as IP addresses or DNS servers. Filippoupolitis et al. demonstrated in their approach that a decision tree can distinguish between bot-based and human attackers [11]. Simmons et al. have developed a taxonomy called "AVOIDIT" that describes cyber attacks using a classifier [12]. Barn, R. and Barn, B. have designed an ontological view of a taxonomy of relationships between relevant cybercrime entities [13]. Kochheim, on the one hand, shows in a structural model that cybercrime meanwhile works according to sources, stages and goals and logistics in a division of labour [14]. In this work, it will be shown how a profile-based approach to cyber attacks leads to the identification of similar or identical cases. In this context, case-based reasoning offers itself through the logic of finding similar cases to similar solutions. For this purpose, the CBR cycles 'Retrieve', 'Reuse', 'Revise' and 'Retain' are run through in order to find similarities to stored cases on the basis of case properties, and to offer and adapt solutions. The aim is to compare current cybercrime cases with stored cases and assign them to a perpetrator or group of perpetrators as a solution. CBR itself is already used in intrusion detection systems [15].

3. Methodology

This section describes the methodology used, which is chosen for this study in terms of the characteristics of the sample cases, the characteristics of the attackers and their classification based on data collection. In this work, the aim is to profile cyber attacks based on existing stored cases. This raises the question of how will a model for case-based reasoning in the field of cybercrime within a domain of knowledge the case data designed. The stored cases have certain attributes that have been identified and extracted based on existing systems and processes in law enforcement. Thus, the attributes such as modus operandi, attack target, interface, attacker and contact are stored in the system for each case, among others. The stored cases are scanned from publicly available sources such as police web portals using a web crawler and stored in the case database in an attribute-to-attribute matching process. Images and descriptions of national and international cybercrime cases were also collected and transferred to the case database. In

addition to the technical storage of the cases, the research work deals with the topics of text comparison with CBR, comparison of data storage algorithms, decentralised storage of cases using distributed ledger technologies, image comparison and text comparison procedures and voice recognition procedures. The evaluation of the individual topics results in a recommended course of action for a cybercrime profiling system in order to compare new cases using CBR with known stored cases as best as possible and to derive profiling from this. Likewise, the aim of the work is to build methods for determining similarity locally and globally. The case base was designed in an object-oriented manner [16].

4. Profiling of cybercrime attacks

In this research work, real cases from publicly available sources are used. For this purpose, attributes were identified in advance by, on the one hand, analysing and evaluating existing and used software for cybercrime case storage on the market with regard to the attributes. On the other hand, textual descriptions from web portals of law enforcement agencies were also qualitatively evaluated and attributes were derived from them.

4.1. Development of a suitable model

To identify the attributes of a model, the digital forensic process of law enforcement is first considered. Digital forensics takes on a central task in solving cybercrime cases in the true sense. Forensic and digital forensics does not differentiate between cybercrime in the narrower or broader sense. In the field of cybercrime in the narrower sense, a higher level of IT competence in terms of expertise and methods is assumed [17]. Police officers are supposed to have an "awareness of cybercrime" so that cybercrime aspects can be recognised at a crime scene in order to act accordingly until IT specialists are available on site. IT forensics (analogously also digital forensics) is described as a process in which science and technology are used to analyze digital objects involved in crime-related events [18]. The goal here is to use the seized digital objects to conduct a criminal prosecution against the perpetrators. The entire process includes both the crime scene work to be carried out on site with the steps. In the process at hand, injured parties, witnesses and suspects are first identified and the. After that, measures have to be prepared for which the digital data carriers are recorded. For this purpose, choice will be documented on a strategy using established methods and tools. If there is a cybercrime case, the presented process is used to investigate the case. For this purpose, the injured parties, witnesses and suspects are first identified. This is also done with regard to the actual goals of the investigative work. In the next step, preparations are made to record the evaluations of data carriers in writing. The definition of a suitable strategy is achieved by means of the selection of established methods and tools. Security-relevant access restrictions and the further processing of the evaluations of digital data carriers must be managed. The next step is the actual data collection. For this, the various formats of the data must be collected, condensed and unified in a uniform format. With this unified format, the data normalized in this way can be transferred to another format that is easier to evaluate. In the subsequent analysis, events are evaluated and correlations are found. In the last step, the evaluations are interpreted and visualized in a suitable format. Based on the process presented, software solutions have established themselves on the market. On the

one hand, there are case management tools that are used to create and manage crime cases. These systems are also called Law Enforcement Case Management Systems. On the other hand, software solutions are used that have been developed for the purpose of forensic investigations. These tools are used to provide digital leads on a case accordingly. When the case is saved, these traces are stored as attribute values. These tools are called digital forensic tools. The digital forensics tools are purpose-built with regard to digital traces and accordingly have a narrow range of functions. The forensics tools are clearly focused on the search for digital evidence. These types of tools have a correspondingly high degree of specialization and thus represent an important sub-aspect within the scope of investigative work. Most forensic tools are also categorized according to cases. What these tools lack, however, are the higher-level aspects such as suspects, witnesses or injured parties. Accordingly, the tools perform a partial task in the context of a cybercrime case. In order to keep track of the different aspects of the investigative work, case management tools are used. Accordingly, in the further consideration for developing a system based on CBR, the case management tools are considered. By means of this classification, software solutions available and established on the market are found. The following software solutions, among others, can be assigned to the class of case management tools: Maltego[19], Kaseware[20], goCase[21], Column Case[22], OSIRT Browser[23], Matrix Investigator.

4.1.1. Extract requirements

An evaluation and comparison of the tools provides functions that are equally or similarly available in all tools and thus flow into the requirements for the system to be developed. When comparing the tools, nine categories can be identified:

1. All cases are stored securely and encrypted in a database.
2. Relationships are shown between cases for investigators by setting bidirectional links between digital case files.
3. Each case file at hand is stored as a digital evidence object in a secure database.
4. Each digital evidence object can be linked to one or more cases to show relationships among cases.
5. Any modification or access to a cybercrime case is logged against a change history to detect unauthorized access.
6. Cybercrime case information is securely shared with designated recipients for team-based collaboration.
7. Custom queries can be performed on the database by specifying ranges of values.
8. Report generation is enabled based on user-defined queries in the case database.
9. Duplicate content in the database is indicated by the system to the user so that proper merging or deletion is possible.

In addition to the system requirements derived from the above tools as common features, the next step is to identify required attributes.

4.1.2. Extract data field

An extraction of real data of cybercrime cases was realized using a web crawler. The web crawler was developed in Java and used the Selenium test framework. In the process, the webcrawler accessed open sources of law enforcement agencies such as mugshot portals on a test basis (see Figure 1). This ensures that the system is designed close to the reality of investigative authorities. Likewise, search fields with corresponding parameters such as "computer fraud" were automatically set on the respective portals to limit the selection to cybercrime cases. After the respective field values have been read out, they are stored in the proprietary database.

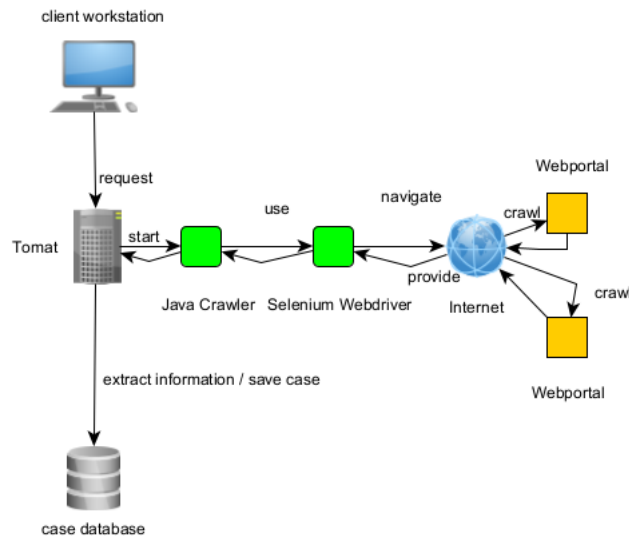


Figure 1: Web crawler

The fields that the web crawler extracts have been defined beforehand using XPath rules. For this purpose, the structure on the respective website was analysed and the set of rules was saved for each attribute to be extracted.

During the development work, the following attributes can be identified on the portals: title, location, zip, authority, offense type, offense start date time, offense end date time, offense description, perpetrator description with sub-attributes like birthday, gender, clothes, physical characteristics, hair color, body figure, media like pictures or videos, contact made by.


Attribute	Description	Example
title	The title attribute briefly states what has happened.	Employees Charged in Hacking Campaigns.
location	The location attribute contains information about the place and locations of the event.	Berlin
zip	A postal code consisting of digits.	12047
authority	Are state agencies that have the task of law enforcement	Police Berlin
offensetype	Specific manifestations of the offence	Computer fraud
offensestartdatetime	Start date and time of the offence	05.08.2022 12:15:00
offenseenddatetime	End date and time of the offence	05.08.2022 14:15:00
offensedescription	Content of the offence	The company was hacked by as yet unknown perpetrator
birthday	The day of birth	13.03.2000
gender	The gender according to female, male, diverse	female
clothes	Means the worn clothes	T-shirt, dark shoes, jeans
physicalcharacteristics	Physical Characteristic means a bodily condition or bodily characteristic of any person	scar
haircolor	The colour of the hair	brown
bodyfigure	It describes the body shape	A wider face
media	Which kind of images, videos, audios	
contactmadeby	How was the contact established	Email

Table 1
Extracted attributes

The attributes of the external portals extracted in this way were incorporated into a class diagram in the further course of the scientific work. The attributes 'title' and 'authority' are assigned to the class Case. The attributes 'location' and 'zip' are added to the Location class. The attributes 'offensetype', 'offensestartdatetime', 'offensenddatetime' and 'offensedescription' describe objects of the class Offense. The attributes 'gender', 'physicalcharacteristics', 'haircolor', 'clothes', 'contactmadeby' and 'bodyfigure' are assigned to the class Perpetrator. A separate class Media is formed from the attribute 'media' (see Figure 2). The object-oriented model created in this way contains classes with the respective attributes and cardinalities. In the class Case the respective cases are represented. An object of the class Case has a solution, which consists of hints and steps. To the case possible witnesses, injured parties and if known offenders are stored. In addition, the case contains media such as extortion letters or telephone calls. A case always refers to at least one object of the class ModusOperandi. An object of the class ModusOperandi contains an object of the class Offense. If determined, Offense also contains a Location object with address data. Likewise a Technology object can be assigned to an object of the class Offense. In addition, the class Case is derived from the class Problem. The reason is to be seen in the Reasoner class itself, since this generically takes cases as parameters in the different methods. The Reasoner class refers to Reasoning, which contains the algorithm for Retrieve. Retrieve, like Reuse, Revise, Retain, and ReasonFactory, is an aggregation of Reasoner.

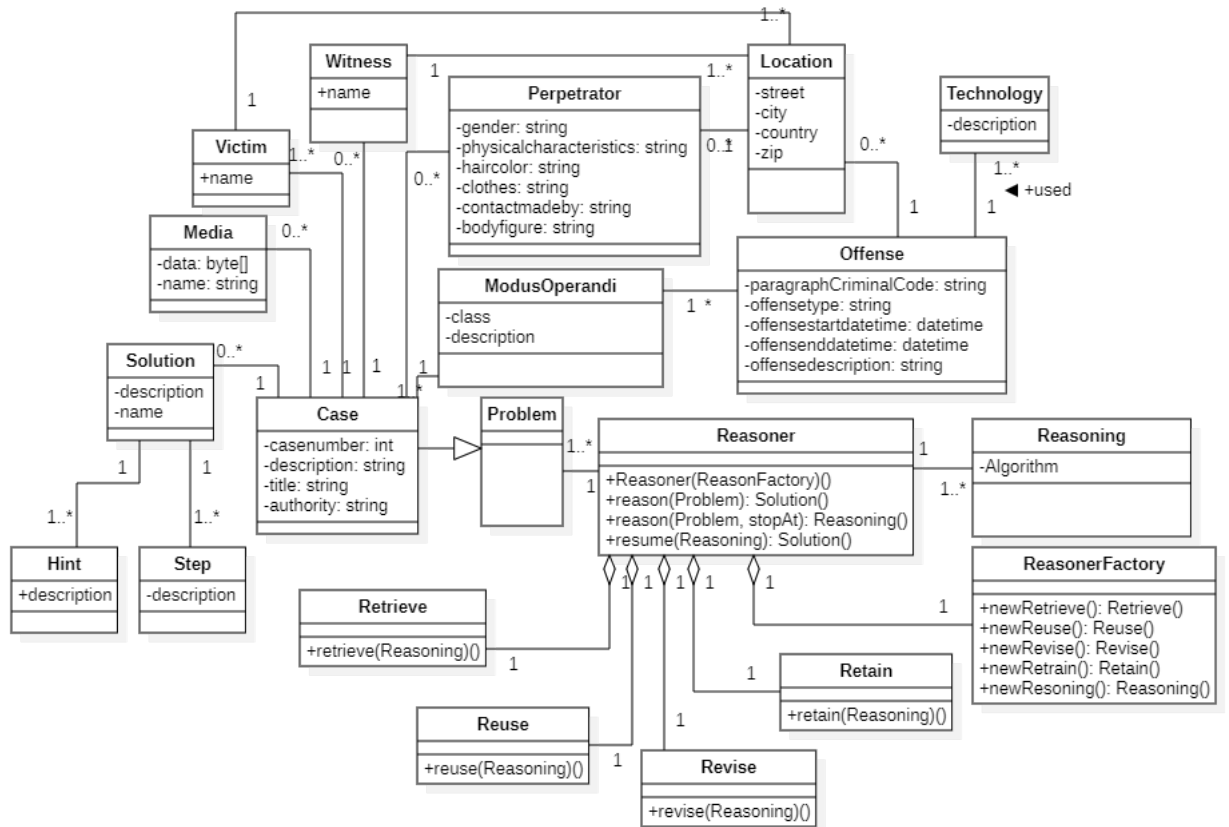


Figure 2: Class diagram

4.2. Text comparison algorithms

In order to perform a similarity determination on the description attributes, different text comparison algorithms were investigated in this research. Thus, for the subfield of text comparison algorithms, 27 cybercrime cases with the respective textual descriptions were stored in the database. Subsequently, twelve cases were selected in order to compare the individual methods for text duplicate detection in a uniform manner. For this purpose, the words of the case descriptions were counted and divided into three categories: Short, Medium and Long. From these, the four shortest and the four longest case descriptions were selected. The four descriptions from the medium-length category were selected from the range around the mean value of 129 words. Different similarity measures and algorithms can be used to identify text duplicates. In this work, the similarity-based methods Hamming distance, fuzzy score, Levenshtein distance, Jaro-Winkler similarity, Jaccard distance, cosine similarity, Monge-Elkan similarity and SoundEx were implemented. The artificial neural networks Word2Vec, Doc2Vec, GloVe and fastText were also compared in the tests. The comparability of the methods was ensured by means of a reference value. This reference value was formed by first manually assessing the similarity of the test data set to the database. For the assessment of similarity, the information such as modus operandi, attack target, attacker or victim in the crime description was evaluated. The similarities were categorised according to the following scheme:

1. The case is identical.
2. The case is similar in more than one keyword.
3. The case is not similar in any keyword.
4. The case is similar in only one keyword.

Thus, a subjective assessment of this categorisation is available. This assessment was done by marking certain key terms in the cybercrime case descriptions. For example, words such as DDoS, service provider, financial institution, bank or customer were extracted. Correspondingly, other cases are considered similar to the reference value if these terms were also used in the case description. A reference case was formed that has the greatest agreement with the other test cases as an overall result. This ensures comparability between the test cases. The methods have already been implemented on a specially developed web application and were available for the ready. In addition to comparing for text similarity, other criteria for evaluating the comparison methods were examined. These were the runtime per comparison run, the implementation effort and the adaptability for own applications. First, the similarity algorithms used recognise an identical case as the most similar case. The comparability of the similarity algorithms with each other is complicated by the fact that the algorithms use very different scales. A one-to-one comparability is therefore not possible. The longer the crime descriptions of a cybercrime case are, the more accurate and "similar" a case is considered to be. In the area of manual similarity assessment, the problem arises that this calculation was made subjectively. To improve the manual similarity assessment, the use of several raters is recommended. Also, the assessment should only be carried out with similar descriptions of the cybercrime cases. The fastText, cosine and Monge-Elkan algorithms have not shown false negatives. The result in the methodological similarity assessment showed that with the highest accuracy Word2Vec calculates the similarity. This is followed by cosine, Jaccard, Monge-Elkan and fastText. With the comparison of the text

comparison algorithms, it can be determined that edit-based methods are not promising. Also, similarity-based methods show a significantly lower computation compared to word embedding methods. Kosinus thus has the best overall result, although this method is not optimal. Rather, a combination of word embedding algorithms and cosine methods would be a more promising possible approach. In advance, it also makes sense to remove identical tokens.

5. Further research and future work

In this paper, a procedure for profiling cybercrime cases using case-based reasoning was presented. The typical attributes of a cybercrime case were identified in order to profile cases using CBR. Some of the attributes are text-based and descriptive, so as the research progressed, the work was extended to text matching algorithms. CBR has proved its worth in the procedures, so it is possible to speak of good results. However, other sub-areas are currently being investigated for cybercrime profiling. These sub-areas include: - Speech recognition of audio files - Image recognition - Algorithms for searching cases from the case base

Comprehensive profiling of cybercrime cases is possible through recognition of speech in audio files, since the text comparison algorithms can be used again with the generated text. In image recognition, different algorithms are tested to recognise identical or similar images. Also, algorithms for searching cases from the case base will be investigated to enable efficient case base searching.

References

- [1] W. E. Forum, Global Risks Report 2019, 2019. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.
- [2] W. E. Forum, Partnership against Cybercrime. Insight Report, 2020. URL: <https://www.weforum.org/reports/partnership-against-cybercrime>.
- [3] Bundeskriminalamt, Cybercrime Bundeslagebild 2018, 2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=3.
- [4] D. Maher, Can artificial intelligence help in the war on cybercrime?, 2009.
- [5] J. Corchado, B. Lees, A hybrid case-based model for forecasting, *Applied Artificial Intelligence* 15 (2001) 105–127. URL: <https://doi.org/10.1080/088395101750065723>. doi:10.1080/088395101750065723. arXiv:<https://doi.org/10.1080/088395101750065723>.
- [6] A. Aamodt, E. Plaza, Case-based reasoning: Foundational issues, methodological variations, and system approaches, *Foundational Issues* 7 (1994) 39–59. doi:10.3233/AIC-1994-7104.
- [7] S. Levy, *Hackers: Heroes of the Computer Revolution*, 1984.
- [8] B. Landreth, *Out of the Inner Circle: A Hacker's Guide to Computer Security*, 1985.
- [9] R. Hollinger, *Computer hackers follow a guttman-like progression*, 1988.
- [10] M. Rogers, *A new hacker taxonomy.*, 2000. URL: <http://homes.cerias.purdue.edu/~mkr/hacker.doc>.
- [11] A. Filippopolitis, G. Loukas, S. Kapetanakis, *Proceedings of the 7th international confer-*

- ence on cybercrime forensics education and training - cfet 2014, in: Towards real-time profiling of human at-tackers and bot detection, CFET, Norwegen, 2014, p. 48.
- [12] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, Q. Wu., *AVOIDIT: A Cyber Attack Taxonomy*, 2009. URL: <https://nsarchive.gwu.edu/document/16663-chris-simmons-charles-ellis-sajjan-shiva>.
- [13] R. Barn, B. Barn, *AN ONTOLOGICAL REPRESENTATION OF A TAXONOMY FOR CYBERCRIME*, 2009. URL: <https://core.ac.uk/download/pdf/42490758.pdf>.
- [14] D. Kochheim, *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*, p. 26, 2nd ed., Verlag C.H. Beck oHG, Munich, Germany, 2018.
- [15] D. G. Schwartz, S. Stoecklin, E. Yilmaz, Proceedings of the 17th int. symp. on computer and information sciences, in: Case-based agents for packet-level intrusion detection in ad hoc networks, Norwegen, 2002, p. 59.
- [16] K. Bach, K.-D. Althoff, *Developing Case-Based Reasoning Applications Using myCBR 3.*, 2012. URL: https://doi.org/10.1007/978-3-642-32986-9_4. doi:10.1007/978-3-642-32986-9_4.
- [17] S. Costantini, G. D. Gasperis, R. Olivieri, *Annals of mathematics and artificial intelligence* 86, in: Digital forensics and investigations meet artificial intelligence, Università degli Studi dell'Aquila, L'Aquila, Italy, 2019, pp. 193–229. doi:10.1007/s10472-019-09632-y.
- [18] A. Shalaginov, J. W. Johnsen, K. Franke, *Ieee international conference on big data*, in: Cyber crime investigations in the era of big data, IEEE, Boston, MA, USA, 2017, pp. 3672–3676. doi:10.1109/BigData.2017.8258362.
- [19] S. Hai-Jew, Real-time sentiment analysis of microblog messages with the maltego "tweet analyzer machine", in: N. Rao (Eds.), *Social Media Listening and Monitoring for Business Applications*, 2017, pp. 316–337.
- [20] J. Deeb-Swihart, A. Endert, A. Bruckman, Understanding law enforcement strategies and needs for combating human trafficking, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, pp. 1–14.
- [21] K. Daka, J. Phiri, Law enforcement case management system (lecms): A case of law enforcement agencies in zambia, in: *International Journal of Advanced Studies in Computers, Science and Engineering*, 6(10), 2017, pp. 30–37.
- [22] R. Ana, V. Ivan, C. Mladen, G. Săvoiu, Knowledge management software application in ice-cream companies, in: Proceedings of the XIV INTERNATIONAL SYMPOSIUM SYMORG 2014, 2014, pp. 1066–1070.
- [23] J. Williams, Open source internet research tool (osirt): an investigative tool for law enforcement officials, in: HEA National Conference for Learning and Teaching in Cyber Security, 2017.