MICHAL BUKOWSKI
ORCID: 0000-0002-5075-8130

COMBATTING ECONOMIC CYBERCRIME USING ARTIFICIAL INTELLIGENCE (AI)

Introduction

Europol\(^\text{2}\) defines financial or economic crime as ‘economic crime, also known as financial crime’.\(^\text{3}\) It refers to unlawful acts committed by a person or group of persons for the purpose of obtaining a financial or professional advantage, the main motive of which is economic (financial) gain. This type of crime includes money laundering, tax evasion, investment fraud, mass marketing fraud and many others. Financial crime has been valued at over one trillion dollars by the World Economic Forum.\(^\text{4}\) There are currently three major organisational structures involved in combating economic crime in Poland. The Bureau for Combating Economic Crime of the Police Headquarters, the Departments for Combating Economic Crime of the Central Bureau of Investigation of the Police, and the Department for Combating Economic Crime of the National Fiscal Administration.

\(^\text{1}\) Lt. Col. EngD Michal Bukowski – since 1997 a police officer, since July 2023 director of the Institute of Criminal Service of the Security and Legal Sciences Department of the Police Academy in Szczecin, previously chief of the Technical Surveillance Department of the Regional Police Headquarters in Gdańsk, chief of the Operational Support Department of the Bureau of Internal Affairs of the Police and deputy chief of the Department of Special Techniques and Execution of the Criminal Bureau of the Police Headquarters. Graduate of the Polish-Japanese Academy of Computer Technology, Cardinal Stefan Wyszyński University in Warsaw and the Military University of Technology.

\(^\text{2}\) The mission of Europol, which is based in The Hague (the Netherlands), is to support Member States in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. Europol also cooperates with a number of non-EU partner states and international organisations. Major criminal and terrorist networks pose a serious threat to the internal security of the EU and to the safety and living conditions of its residents. The greatest threats to security arise from: terrorism, international illicit traffic in narcotics and money laundering, organised fraud, euro counterfeiting and human trafficking. Electronic source: https://www.europol.europa.eu, accessed: 28.03.2023.


Nowadays, financial crimes committed in cyberspace are always committed using both hacking tools and all kinds of tools using socio-technical methods. They bypass all possible safeguards, including those of government financial institutions and various types of corporate institutions. This behaviour leads to different types of financial crime being viewed in an unequal light. The distinction between financial crime, hacking and social engineering used for economic and financial gain has become blurred.

Technological advances, technical skills and wide-ranging practical experience are available to both criminals and law enforcement agencies. For the latter, unfortunately, there are major financial constraints that lead to an inability to eliminate organised crime groups. Understanding the tactics of committing crimes and the methods and techniques used to combat them is becoming more difficult by the day.

Many authors of professional literature describing the cybercrime industry describe it as a 21st century challenge, as it is in line with increasing digitalisation, financial change and the explosion and expansion of the popularity of cryptocurrencies. This symbiosis of financial crime and cybersecurity guarantees leads financial institutions to use methods they have developed to protect their assets using real-time analytical tools that guarantee the interception of, for example, network attacks, and thus prevent financial losses. However, there are security models that show a lack of ability to prevent such attacks and algorithms to deal with such attacks. Analysts recommend the development and implementation of state-of-the-art methods in various organisations to prevent further business losses, as well as the loss of customer data and corporate reputation. New methods being implemented in academia and industry are machine learning and deep learning models.

In order to combat economic cybercrime, special attention must be paid to Anomaly Detection (hereafter: AD), which is one of the methods used to identify financial criminals online and to detect and prevent the occurrence of illegal financial transactions. With the increasing technical capabilities and ingenuity of cyber criminals, as well as evolving tools for masking identities, it is becoming increasingly difficult to protect both public and private assets. Group Anomaly Detection (GAD) is the next step in detecting anomalies that are generated by a criminal using multiple false identities or that he or she generates through collaboration with an organised crime group.

Background

In attempting to present the fight against economic cybercrime using artificial intelligence (AI), there is a need to present anomalies as a means

---

of detecting economic crime in cyberspace. There is also a need to briefly characterise the anomaly detection and deep learning methods that are used to draw the attention of law enforcement towards uncovering criminal activity.

**Types of anomalies**

An anomaly is nothing more than something very rare, strange, deviating from a certain norm, often unnatural. In science, an anomaly is a deviation from the average or an observation that deviates from other observations. We divide anomalies into point, contextual, and collective.

**Point anomaly**

A point anomaly is nothing more than a point in a data stream that stands out from the rest of it, often referred to as an outlier. Figure 1 illustrates a point anomaly.

![Data series with point anomaly](source: own elaboration)

---

8 Aggarwal C.C, Outlier analysis in Data Mining. Cham, 2015, pp. 237–263.
Contextual anomaly

A Contextual Anomaly is a point that is normal at some specific point in time, but abnormal at another point in time. Such an anomaly requires knowledge of the context, or normal behaviour. It is also called a conditional anomaly.\(^9\) This type of anomaly is common in data streams generated for time series. For example, a high volume of traffic at a boom barrier for cars entering a fenced property is normal before or after the start of work, but in the middle of the working day, for example, it is contextually anomalous behaviour. Such a situation could arise as a result of, for example, a fire or building disaster. In the case of this type of anomaly, we must also analyse other dependent parameters that will enable us to consider the deviation from the average as an anomaly or to qualify it as typical behaviour.

Figure 2 shows an example of a contextual anomaly.

Collective anomaly

A Collective Anomaly can be detected by analysing a data stream to determine its collective normal behaviour. Any deviation from the normal

pattern can lead to a collective anomaly in relation to whole patterns of data following consecutive specified time intervals. For example, a single observation in an interval is not sufficient to determine the behaviour of the heart, whereas collective signals can determine normal or abnormal behaviour, as shown in Figure 3. It can be seen here that the pattern of observations is anomalous in the third peak of the heartbeat, indicated by the red ellipse, at precisely the time of rest – an extended time, compared to the rest of the recorded signals (data sequence). Any kind of collective anomaly is related to the time unit, while it is possible to have seasonal trends in such data streams. For example, a heart rate signal may be anomalous due to a reading just after a run or physical activity. Similarly, ice cream sales increase during the summer and decrease at the end of the summer season. We can also observe the seasonal effect in the consumption of natural gas volumes, which increases in winter and decreases in summer.

Anomaly detection

Anomaly detection involves the use of computational thinking (computational) and mathematical (computational) techniques so that it becomes possible to detect anomalous points (anomalies) in a dataset. The literature refers to anomaly detection as spur detection, novelty detection, noise detection or deviation detection, and defines it as the process of analysing a dataset to identify instances of deviation. It includes:
— identification of anomalous data, e.g. noise, deviations or outliers from the original dataset,

---

— discovering new data instances based on the acquired knowledge of the form of the original dataset. We can use anomaly detection for:
— fraud detection,
— data quality analysis,
— security level scanning,
— status monitoring of processes and systems,
— monitoring of static images and video sequences,
— spam detection,
— detection of malicious attacks,
— data cleaning before training statistical models and neural networks,
— analysis of human behaviour,
— sensor fault detection.  

**Detection of group anomalies**

Group anomaly detection (hereafter: GAD) is a technique for identifying sets or clusters of data points that are abnormal or inconsistent with a group pattern. Like traditional anomaly detection, GAD addresses the problem of finding patterns in groups of data that do not conform to our expected behaviour. Group anomalies can consist of individual anomalous points, which are relatively easy to detect, arising around a normal group, and anomalous groups arising around relatively normal points whose behaviour as a group is abnormal, which is much more difficult to detect by any method. The concept of detecting group anomalies is divided into dynamic and static situations. Static GAD identifies such groups that are at odds with normal group behaviour, while dynamic GAD investigates differences in the group state over a period of time.

**Group anomaly detection methods based on networks or graphs**

Networks or graphs play an important role in GAD and, in particular, when attempting to detect them in relation to crimes committed using cyberspace. State-of-the-art research and published algorithms include a pre-processing step or direct analysis of graph or network structures to identify anomalous clusters or social groups. Due to the variety and mix of different types of networks and graphs available in actual searched models, it is crucial to use application-specific properties to define anomalies that may occur in networks or graphs. We can define outliers in networks as nodes, edges, subgraphs or subgroups. Spatio-temporal graphs have exactly the same anomalous values, except for the evolving and dynamic

---


nature, which generates additional difficulties in identifying these values. Methods based on networks or nodes make it possible to detect group anomalies in Big Data, social networks, banking networks, chemical compounds, and knowledge graphs such as the citation network, bibliography network and many other areas of life and science.

**Deep learning**

Deep Learning (hereafter: DL) is a sub-discipline of Machine Learning (hereafter: ML) that uses artificial neural networks to learn representations or features of an input dataset. As with graphs, DL plays a key role in the future of AD and GAD. The advantage of using deep learning models is that neural networks can learn their own connections to specific data points through a back propagation method. This allows individual input data to be weighted differently across the input data set. This bypasses the need to manually detect anomalous features.\(^\text{16}\) However, the back-propagation method typically uses gradient descent methods as the form of the loss function, and this may result in the loss minimisation not reaching the optimal point due to the fact that the loss function surface has many local minima and the global minimum may not be discovered. The types of DL models are autoencoders, Recurrent Neural Networks (hereafter: RNNs) and Graph Neural Networks (hereafter: GNNs). There are hybrid models that are a mixture of DL and ML\(^\text{17}\) using a Deep Belief Network (DBN) trained to extract the essential features, and then a single-class Support Vector Machine (SVM) trained on the features extracted by the DBN model.

The types of anomaly detection surveillance focus on ground truths and the ability of the models used to correctly classify anomalies with the information they have. These types are:

— Supervised anomaly detection – models require accessibility to labels for definitions of normality and abnormality,
— Semi-supervised anomaly detection – only normal data samples or only abnormal data samples are used as input; the algorithm attempts to model a single concept and detects the anomaly depending on the condition of the data used in building the concept,
— Unsupervised anomaly detection – used when there is no prior knowledge of the dataset and label information is not known,
— Human-in-the-loop – active learning corresponds to a configuration in which the learning algorithm can selectively query the human analyst for input instance labels to improve its prediction accuracy.


Currently, AD is moving towards the simultaneous use of graph models and deep learning algorithms, which has been called GNNs. Examples of GNNs include Recurrent Graph Neural Networks, Graph Convolutional Networks and Spatio-Temporal Graph Neural Networks.\textsuperscript{18}

**Actors and victims**

In the UML language,\textsuperscript{19} an actor is a user or external system with which the modelled system interacts.\textsuperscript{20} In this paper, we will use the word ‘actor’ in the sense of a cyber actor. To understand the anomalous behaviour generated by actors, we need to deepen our understanding of their typical actions by studying social patterns and their psychological characteristics. Actors are constantly adapting their methods of action to maintain their powerful position in the ecosystem they have created.

**Actors and their typical activities**

**Trust**

Social psychologists and neuroscientists describe trust as an effective mechanism used by humans to cope with complexity, especially in situations of risk and uncertainty. There are few areas of modern civilisation that are a greater breeding ground for uncertainty than the underworld associated with cybercrime. It is important to be aware that actors rarely commit crimes against individuals they know in real life. Successful actors are well aware of the importance of trust, understanding that they need to convey elements of familiarity, similarity and technical knowledge to encourage the ‘successful’ behaviour they assumed at the outset of their activities. It is important to bear in mind that – when an actor loses trust – he or she is quickly removed from the operation in question.

**Shining by example**

Experienced successful actors demonstrate remarkable abilities in making effective judgements and decisions. They often reflect effective, legitimate leadership qualities – they are effective managers, decision-makers and problem-solvers because they follow the strict rules that govern them and their teams. They also demonstrate authority by delegating tasks while managing their team’s expectations and attracting capable,


financially motivated and highly skilled partners. These actors often cut through the hype among their peers and the media, focusing primarily on the financial gains they make.

Adapt or perish

When disruptions to an actor’s operations occur – such as patching security vulnerabilities, leaking source code or disrupting infrastructure – how they deal with these changes can make or break their long-term success. It has been observed that high-performing cybercrime groups repeatedly develop new malware and restructure teams and operations dynamically to meet emerging needs. The most successful actors are often first recognised in the media or by elite researchers and they pioneer certain attack methods, before others are quick to copy their actions. Whether they are good at thinking for themselves, pondering the future, or switching to alternative plans, these actors know that change is constant and necessary, and such behaviours guarantee increased profitability.

Faceless

Successful actors use all possible layers of anonymity that the Internet provides to hide their true identities. Greater anonymity guarantees greater security. The difficulty of identifying an actor increases the chances that they will not be caught and judged. However, those actors who want to succeed must strike the right balance between being sufficiently well known, thus gaining credibility, and being hidden. Those in the underground who balance this tend to implement better security practices (OPSEC\textsuperscript{21}), such as using email addresses and accounts unrelated to personal accounts, so as not to be linked to a real identity in any form. They also try to avoid revealing personal information when chatting on forums, chat rooms or social media.

Actors use a variety of tools, such as bulletproof hosting services\textsuperscript{22} (BPH), Tor browsers\textsuperscript{23} and VPNs,\textsuperscript{24} to protect their infrastructure and identities. Actors also anonymise their funds and transactions through cryptocurrency blending services. They attempt to make cryptocurrency funds and transactions untraceable, making the actor’s profits less likely to be tracked by law enforcement.

Such strategies and tools are not always enough to allow actors to remain anonymous. Successful cybercriminals monitor how much attention they


get and know when to hide. Usually, they come back with a new alias and an improved strategy of operation, which guarantees they will remain safe. If they do not return, it means they are starting to use the ‘earned’ funds.

**Easy to do**

Actors of all skill levels choose the easiest possible path to make money. The successful ones engage in active scanning – a process that is extremely easy to set up and automate – to successfully attack organisations by exploiting entities with unpatched vulnerabilities. This is then accompanied by brute-force attacks and pushing credentials onto subordinate systems to gain access to the network. Such a process underpins many of the actors who are known as the top network access brokers in the cybercrime underground. Their business strategy is to sell large volumes of access to global organisations in various sectors to attract multiple buyers. This tactic has been adopted by many other actors, who appear to attack any organisation they can easily gain initial access to, rather than spending time and effort attacking specific organisations. Some of the most successful actors have used these strategies and outsourced ways to gain access, even going so far as to employ penetration testers to gain access to their own programmes.

**Knowledge is power**

High-performing cyber actors are often inquisitive and lifelong learners. They are proficient in technology, seek out mentors, enrol in legal and illegal courses, follow technical media, attend lectures and explore new areas of science and research. Training courses, step-by-step guides, manuals and video presentations enable these actors to raise their level of skill or sophistication. Whether purely technical or rooted in social engineering, the constant pursuit of knowledge helps them to successfully achieve their goals.

**Organised crime**

Over time, cybercrime networks have become more organised, collaborative and well-funded. Highly skilled actors are growing their businesses and reinvesting some of the earnings back into their ventures. As with other professional business ventures, cyber actors are reinvesting profits back into the illegal venture to improve their capabilities, infrastructure, platforms and offerings. This expands their ability to hone their technical skills and enables more sophisticated attacks. Over the past decade, there has been a marked shift in the way these actors handle their activities. In general, cybercrime groups view the negotiation and methodologies of attacks with a business mindset, particularly with regard to the professionalisation of their services and the way they communicate. Rather than reacting emotionally, they approach interactions with standard operating
procedures and clarify partners’ expectations early and often throughout the relationship.

Victims

We are all human beings with our own unique quirks, flaws and behaviours, which actors notice and exploit. With the constant development and transformation of technology, they have several types of activities at their disposal that they can use to their advantage. They use our identifiers, tendencies and inclinations to gain access to the things we value most and whose safety we care about.

Here are some of the most common human behaviours used by actors to carry out all kinds of malicious attacks or commit criminal acts.

Curiosity

People have a natural tendency to explore and solve puzzles. Phishing scammers take advantage of this by sending malicious links that take unsuspecting users to crafted websites or allow them to download dangerous software.

Credibility

People tend to trust sites and emails that look familiar and authentic, so scammers hide their sites from unsuspecting users under the guise of a government or corporate site.

Loose safety habits

Most people tend to use the same passwords or use weak passwords, making it easy for cybercriminals to guess them and gain access to accounts and take over sensitive information.

Attention to detail

People often omit details and do not read the fine print in web forms. Cybercriminals know this and take advantage of it, moreover they fill in the missing information themselves to gain access to user accounts and data.

Lack of awareness

People often lack cyber security awareness and are easily fooled by seemingly trustworthy digital entities such as websites and emails. This lack of vigilance is exploited by cybercriminals to run malware and gain access to personal data.
Financial cybercrime

Cyberspace provides many opportunities for criminals – attacking individual computers, networks, critical infrastructure, or holding money or data to ransom. It facilitates crime and large-scale fraud and globally affects national security. Today, it is already clear that cyber risk is in fact business risk, and cyber security is national security. In 2022, the FBI’s Internet Crime Complaint Center (IC3) received 800,944 complaints with a total financial loss of more than $10.2 billion. The FBI report also detailed the number of complaints and victims, the wide range of crime types used and the reported amounts of money both stolen by criminals and subsequently recovered by the FBI Recovery Assets Team (RAT). Table 1 shows the number of victims for selected crime types reported in the US in 2022, and the amounts stolen using this method (a total of 27 crime types were reported). The largest value of criminal activity reportedly came from investments totalling more than $3.3 billion. This report highlights the huge amounts of money that can be extorted from victims of financial cybercrime.

Table 1
Number of victims of selected crime types reported in the US in 2022 and amounts stolen using this method

<table>
<thead>
<tr>
<th>Type of crime</th>
<th>Number of victims</th>
<th>Lost funds in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>300,497</td>
<td>52 million</td>
</tr>
<tr>
<td>Acquisition of personal data</td>
<td>58,859</td>
<td>742 million</td>
</tr>
<tr>
<td>No payment/no delivery</td>
<td>51,679</td>
<td>281 million</td>
</tr>
<tr>
<td>Financial extortion</td>
<td>39,416</td>
<td>54 million</td>
</tr>
<tr>
<td>Technical support</td>
<td>32,538</td>
<td>806 million</td>
</tr>
<tr>
<td>Investments</td>
<td>30,529</td>
<td>3,311 million</td>
</tr>
<tr>
<td>Identity theft</td>
<td>27,922</td>
<td>189 million</td>
</tr>
<tr>
<td>Credit cards/cheques</td>
<td>22,985</td>
<td>264 million</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>21,832</td>
<td>2,742 million</td>
</tr>
</tbody>
</table>

*Source:* own compilation based on FBI report (see footnote 25)

Perpetrators of financial cybercrime are difficult to identify. They deliberately mask their activities to blend their actions into the normal behaviour of any other customer or user of a financial website or service, but when the activity is grouped together, the abnormality is more apparent.

---

Investment fraud

Securities (shares, pre-emptive rights, rights to shares, subscription warrants, depositary receipts, bonds, mortgage bonds, investment certificates, other transferable securities, other transferable property rights) allow people to invest their money with a view to making a profit based on research or simply a hunch. However, some market participants have been known to cheat and thus make huge profits at the expense of institutional and retail investors, with the latter suffering losses. Catching such fraudulent actors is not easy and usually requires the involvement of a large number of staff, who are forced to collect evidence of the frauds committed over a long period of time. However, recent developments in machine learning applications and techniques are helping to identify actors in a more efficient and faster way. Some of the methods used by those committing fraudulent investment activities include manipulation, insider trading, money laundering or terrorism.

Manipulation is nothing more than the act of selling or buying a financial security in order to intentionally manipulate the price of the underlying asset or security. Illegal insider trading or insider dealing occurs when ‘insiders’, i.e. persons with access to a company’s private and non-public material, use this information prior to public dissemination for monetary gain. This includes not only the trading of securities, but also the disclosure of non-public information to third parties.

In the field of machine learning and deep learning, progress has been made in addressing these two areas. The methods developed in recent years for training and using neural networks can help detect groups of insiders or co-conspirators in relation to insider trading. These algorithms are also able to identify potential market manipulation by analysing a stock order book to uncover links of traders or brokers acting in an unusual (anomalous) manner that would be contrary to the benefit of their clients or the wider investor market.

One algorithm is an RNN-based ensemble learning system for detecting stock price manipulation. A training set was built from cases downloaded from the China Securities Regulatory Commission with corresponding financial data. A further development of the proposed algorithm is the use of time series analysis methods for stock trading data using LSTM.²⁶ The use of LSTM also provides the opportunity to analyse the social relationships of company executives and the content of announcements, which will significantly improve the ability to detect manipulation with the ability to identify insider trading.²⁷

²⁶ Long short-term memory, LSTM – a type of RNN.
Money laundering

A method used by criminals or those in possession of ‘dirty’ (illegal) funds obtained most often through criminal activity to introduce them into the legitimate economy. The Crown Prosecution Service (CPS) in the UK\textsuperscript{28} defines a money laundering scheme as typically involving three stages. The first stage is the placement of dirty money, which is the process of depositing the proceeds of crime in some financial system. The second stage is layering, which is the movement of money within the financial system through complex networks of transactions in order to conceal it. This layering is usually carried out through offshore companies. Finally, the third stage involves integration, which involves absorbing or infusing the criminal money into the real economy through investments such as real estate, or purchasing shares or luxury items.

Machine learning and deep learning have gained popularity in the fight against money laundering and attempts to identify illegal transactions using online social networks and cryptocurrencies. Paweł Opitek\textsuperscript{29} has written about anti-money laundering using virtual currencies in light of national and international anti-money laundering (AML)\textsuperscript{30} regulations, while one of Asia’s large social networks has a digital currency on its network, allowing users to transact with other users to make purchases and also to transfer the digital currency to others online. One of the problems with this service is precisely the laundering of digital currency.

DNN\textsuperscript{31} was used to detect laundering accounts. Initially, around 500,000 accounts were selected and flagged as benign or malicious by tracking advertisements for cheap virtual currency in the main online shops available. An analysis of the websites visited by the owners of these accounts was then performed and logins were associated with IP addresses to further identify malicious activity. Features were designed to identify account behaviour such as certain types of account activity, such as photo uploads or engagement on a site outside of finance, methods of topping up digital currency, withdrawals, spending and donations. Financial activity sequences were modelled using a discrete-time Markov chain model. The captured sequences were used as features in the model. These features were then loaded into a graph, which was used as a global overview of currency transfer behaviour between accounts. Subgraphs that


\textsuperscript{29} Opitek P, Przeciwdziałanie praniu pieniędzy z wykorzystaniem walut wirtualnych w świetle krajowych i międzynarodowych regulacji AML, \textit{Prokuratura i Prawo} 2020, No. 12, pp. 41–70.

\textsuperscript{30} Anti-money laundering and counter-terrorist financing system. The Polish anti-money laundering and counterterrorist financing (AML/CFT) regime is primarily shaped by both domestic and EU (EU) regulations. The basic legal act in this respect is the Act of 1 March 2018 on Anti-Money Laundering and Financing of Terrorism (consolidated text Journal of Laws of 2023, item 1124); AML/CFT. \textit{Electronic source: https://www.gov.pl/web/finance/aml-cft, accessed: 09.05.2023.}

mapped malicious to malicious, benign to benign and malicious to benign accounts were then identified using the Fast Unfolding method,\(^\text{32}\) which finds social structures in large networks. Statistical classifiers were used to identify malicious accounts in the created features. SVM, random forest and logistic regression classifiers were used. These gave very high accuracy results (TP – True Positive) of 94.2% with a very low false positive rate (FP – False Positive) of 0.97%. Information gain metrics were extracted from the features to identify their relevance to the designated model. The best features included the percentage of gift spend in the community and normalisation of the number of target accounts in the community. The top five extracted features, all with information gain > 0.5, were extracted from the adopted model. Without the use of group anomaly detection methods, such as Fast Unfolding, to detect subgroups in the overall social network community, the accuracy of the adopted model would have been compromised, as the features with the highest information gain would not have been included.

Criminals create organisational structures with a view to obfuscation.\(^\text{33}\) To combat them, it is necessary to identify entire networks in order to understand and define the roles of their individual members. By integrating algorithms, performing social network analysis\(^\text{34}\) and using data from bank accounts and the national court register, social networks are being constructed and analysed during AML investigations. The researchers were able to identify key elements of money laundering rings. They were able to uncover the true leaders and their vulnerabilities. They were also able to detect which accounts are held by the same person. The clustering techniques implemented made it possible to find and assign specific roles to individuals in the network. The implication is that combining machine learning techniques with social network analysis can be a powerful tool in determining crime networks and anti-money laundering. These tools, when combined with people in the loop, such as law enforcement or AML specialists, can produce very accurate and promising results.

**Cryptocurrencies**

According to CipherTrace,\(^\text{35}\) as reported March 2023, losses through the seven main methods of cryptocurrency hacking, fraud or theft reached

---


\(^{33}\) Obfuscation – code obfuscation. It is a technique for transforming programs that change their syntax but retain their semantics, making them significantly more difficult to understand. There are 3 types of obfuscation transformations: layout transformation, data transformation, control transformation. *Electronic source*: https://en.wikipedia.org/wiki/Obfuscation_(software), *accessed*: 09.05.2023.


$383 million in the US, while at the end of Q3, the total market capitalisation of all cryptocurrency assets, including stablecoins and tokens, was around $1.1 trillion. As recently as 2019, Decentralised Finance (DeFi) fraud was rare, while today it accounts for around 70% of the total volume of fraud and theft. Money laundering and terrorist financing are enabled precisely by the use of cryptocurrency. The main criminal entities operating in the cryptocurrency industry are:

— the largest English-language darknet marketplaces, these include: AlphaBay, ASAP Market and Bohemia (AlphaBay was the largest darknet marketplace in 2017 with over 400,000 users before the site was taken over on 5 July 2021. Desnake, a former AlphaBay administrator, appeared on a crime forum to announce the relaunch of the marketplace. The new AlphaBay is more focused on security, especially as the marketplace is exclusively based on Monero. In mid-September 2022, AlphaBay’s reported statistics on the number of buyer accounts on the site exceeded 1 million. If true, this would be one of the largest marketplaces of its kind. AlphaBay is now the largest Monero-only darknet marketplace, beating Monopoly Market, which was originally a Monero-only site but eventually succumbed to user pressure and accepted bitcoin).

— the largest darknet markets of the Commonwealth of Independent States (CIS) region, these are: OMG!OMG!, Shkaf, o3shop, Mega and BlackSprut (Currently, competition in the darknet markets in the CIS region has increased significantly, mainly in Russia. CipherTrace researchers consider OMG!OMG! to be the most significant Russian darknet market currently operating).

The most prominent active fraud operators are: Benumb, Biden Cash, Brians Club, Genesis Market, HGN01 and Rescator. Most of these are carding sites, while Genesis Market is a long-established ‘bot’ marketplace. Carding sites help buy and sell stolen credit card information. Often the larger carding sites are autoshops. An autoshop is a carding site that allows buyers to check if a stolen card is still active and, if it is not, automatically receive a refund. Genesis Market bots refer to digital identities for sale. Genesis Market mainly sells cookies, digital fingerprints, stolen login details, etc., to help criminals impersonate people and gain access

36 Dark web (net), dark web – a term used to describe a deliberately hidden part of the Internet’s resources that can only be viewed using special software. The Dark web can be accessed from the so-called Darknet, consisting of many distributed, anonymous nodes (e.g. Tor, I2P or Freenet). Electronic source: https://en.wikipedia.org/wiki/Dark_web, accessed: 09.05.2023.


38 Carding is a term describing the trafficking and unauthorised use of credit cards. Stolen credit cards or credit card numbers are used to buy prepaid gift cards to cover the actors’ tracks. Activities also include the use of personal data and money laundering techniques. Modern card sites have been described as full-service commercial entities. Electronic source: https://en.wikipedia.org/wiki/Carding_(fraud), accessed: 09.05.2023.
to their accounts. Typically, more than 400,000 different digital identities are put up for sale at any one time.

Cryptocurrency mixing/tumbling is a method used by cybercriminals to launder cryptocurrencies through different wallets in order to disguise the origin of the funds. This is done by using a trusted third party to receive the cryptocurrency from the original address and using an alternative address to send the original funds to the user’s newly created address. This is also done through multiple addresses to create a difficult trail to map back to the original address, which in turn could identify the person.

**Deanonymising Cryptocurrency Blockchains (DCBs)**

To combat financial crime taking place in cyberspace, it is essential to be able to identify the controllers of cryptocurrency accounts. As the use of cryptocurrencies begins to grow, lawmakers have enshrined in law the need for some cryptocurrency exchanges to practice AML. This includes implementing a Know Your Customer (KYC) requirement across the entire user base. The paper Deanonymizing cryptocurrency with graph learning: The promises and challenges describes an approach to deanonymising bitcoin blockchains through the use of GCN. It also describes details of the characteristics of large networks that can be used to train DNNs to detect anomalies, viz:

— large and extremely skewed graphs,
— dynamically growing graphs,
— semantic graphs.

Semantic graphs describe the various activities that blockchain can be used for, including, for example, concluding smart contracts. With GCN, it is possible to:

— detect addresses that are inactive or have a zero balance,
— detect publicly available address labels.

GCN is able to reduce the graph size by identifying inactive/zero balance addresses, resulting in a reduced graph for better computation speeds. The aforementioned advantages of GCN, due to some exchanges or websites that may require KYC, enable identification of portfolio identities.

**Customs fraud**

Customs fraud is the evasion of payment for the importation of goods into a country. It is not a crime committed solely in cyberspace, but it is a financial crime that is also being tackled using machine learning. The EU

---


anti-fraud office\textsuperscript{41} has found that customs fraud is financially damaging to legitimate industry and the EU taxpayer. Between 2010 and 2021, the EU antifraud office recovered a total of €8 billion from over 2,400 customs fraud investigations (2021: 212 investigations totalling €527.4 million – with a budget for its activities of €61 million). Due to the huge volume of transactions and the manual inspection of goods required for customs fraud investigations, it is not possible, without committing huge resources, to screen every single good imported into a country.

There are advances in communities using artificial intelligence for research, aiming to create systems to help customs fraud officers detect imported goods that need to be subjected to a detailed inspection (search). A scenario\textsuperscript{42} of human-assisted customs selection was investigated. The data entered into the model were the import declaration forms required by customs. The selection model highlighted goods that it thought should be inspected by a customs officer, and the officer provided feedback to the selection model, accepting or rejecting the potentially suspicious declaration form identified by the model. In the case of tax evasion, and more specifically customs evasion, the issue of revenue generated by the inspection and identification of evasion was a target that was taken into account in the modelling. The main model used in the research by Sundong Kim, among others, was the DATE model. This is a tree-based dual-attentive model that allows for the optimisation of dual targets. In this case, the dual objectives were both the classification of illegal transactions and the prediction of revenue return. An exploration strategy and an exploitation strategy were used to search for the best model in the selection process. An exploration strategy is defined as an approach to select uncertain positions at the risk of immediate revenue loss, with the potential to detect more novel fraud patterns in the future. The exploitation approach seeks to select the most likely items associated with fraud and high returns to secure short-term revenue for customs administration. The data set collected for this experiment used transaction-level import declaration information from three African countries. These declarations were highly accurate, including the amounts of duties charged, due to the almost 100% inspection rate of imported goods. A number of hybrid techniques were implemented, but the main model used in the selection process was DATE, showing the highest evaluation performance.

Tax evasion

Tax evasion is the unlawful action of taxpayers in deliberately failing to pay their tax obligations to the relevant authorities. There are a significant


number of studies that have taken place in the field of tax evasion using deep learning and machine learning, e.g. research done on Bulgarian taxpayers or traders,\textsuperscript{43} who were in default of their VAT obligations. Experimenting with a dataset of Bulgarian taxpayers and traders totalling 312,726, with an average of 75 per cent of them carrying out one financial transaction per month, the researchers identified a high (in the order of 80) percentage of non-compliant taxpayers/traders within Bulgarian VAT returns and books.

**SIM-Swapping**

SIM-Swapping is an attack that allows a cybercriminal to gain unauthorised control of a wireless customer’s mobile phone number. This gives the attacker access to SMS-based text messages to reset account passwords on websites that rely on mobile number security.\textsuperscript{44} A successful SIM-Swap attack requires the actor to have the target’s phone number and, depending on the account they want to access, also their email address. Actors will either contact the victim’s service provider and mimic them in order to transfer the phone number to a new SIM card, or they have cooperating employees within the service provider, providing them an easier access route. Once the actor has access to the victim’s phone number on their own SIM card, they can extract SMS messages, including one-time passwords sent by financial services or banks. The diagram of the SIM-Swap process is as follows:

- **Phase 1:** The attacker gains access to the victim’s account credentials and mobile phone numbers.
- **Phase 2:** The attacker manipulates the service provider into performing a SIM-Swap with the victim’s mobile number.
- **Phase 3:** Using the newly gained access, the attacker can now use the credentials to initiate a login attempt to the financial account.
- **Phase 4:** The financial service provider sends a one-time password to the victim’s mobile phone number.
- **Phase 5:** The victim’s financial account is accessed and funds are transferred and laundered.

Researchers’ studies have identified three main stages in the crime of SIM card swapping: 1) the theft of personal data, 2) fraudulent copying of the SIM card, and 3) the use of a fraudulently obtained mobile service to commit a crime. Research has also shown that the subscriber authentication procedure associated with SIM swapping is vulnerable to identity


Theft, especially in countries that have implemented eSIM. Relevant to this type of crime was the work of researchers analysing the 2021 hack of the T-Mobile mobile network by John Erin Binns, which resulted in the theft of the personal data of 54 million customers. The attacker accessed T-Mobile's billing systems via a router that was not properly secured and used brute force techniques to gain access to sensitive information stored on the company's internal servers. The stolen data included names, addresses, national insurance numbers, birthdays, driver's licence numbers, identification information, IMEI and IMSI numbers. The aforementioned study outlined how the acquisition of the above data opens the door to identity theft and many other forms of hacking, such as SIM card takeover. Research has also been conducted into the ease of obtaining mobile phone numbers via various communication services such as WhatsApp, Signal and Telegram. In the publication All the numbers are U.S.: Large-scale abuse of contact discovery in mobile messengers, the authors described the use of mobile messenger contact discovery and mobile phone mining methods and how to obtain their private data. Through a combination of crawling and hash reversal attacks, in a fixed time frame and with limited resources, the researchers were able to obtain 100% of mobile phone numbers for Signal, 10% for WhatsApp and expose weaknesses in the Telegram API, revealing a wide range of sensitive information. Such security and privacy vulnerabilities in messaging apps allow potential attackers to access and identify victims for SIM-Swapping.

Phishing

Phishing is considered a social engineering technique that involves getting the victim to provide their personal information, including passwords, email addresses, phone numbers, addresses, usernames and financial information. Analysing Table 1, above, it is reported that phishing and its variants led to $52 million in losses in the US in 2022 alone. In 2020, a tool called SEADer++ was developed to detect social engineering attacks in online environments using machine learning. This system attempts

---


to detect social engineering attacks based on NLP and artificial neural networks. The researchers based their concept on an attempt to detect a social engineering attack in an online chat environment. The proposed process consisted of three steps, which were data preprocessing, feature extraction and result aggregation. The aggregation of results included a classification technique to identify social engineering attempts. The researchers noted the high accuracy of the classification results using decision tree, random forest and MLP. Based on the AUC results, the proposed Soft-voting Ensemble Learning method was found to be the best solution for an industrial application. Understanding the psychology behind social engineering and its ability to manipulate people can help in the fight against phishing. As seen in the SEADer++ tool, the principles of persuasion and psychomanipulation have been used. The paper Human Cognition Through the Lens of Social Engineering Cyberattacks\textsuperscript{50} proposes treating social engineering cyberattacks as a psychological attack and suggests extending the standard framework of human cognition to recognise and accommodate social engineering cyberattacks. This framework created by the researchers led to a quantitative representation of the mathematical characterisation of persuasion. This work demonstrates the breadth of science and research needed to effectively combat sociotechnical cyberattacks targeting industry and civilians.

**Fraudulent romance**

Romance fraud as defined by the FBI\textsuperscript{51} is a scam that occurs when a criminal assumes a false identity online to gain the victim’s affection and trust. Fraudsters use this trust to build the illusion of romance or a close relationship and manipulate victims for financial gain. This type of fraud has seen an increase in popularity among criminals particularly as a result of the global lockdowns caused by COVID-19 – with reports of up to a 20% increase in bank transfer fraud associated with romance scams in 2020 compared to 2019. Victims are not only robbed of their own money, but can be used as money laundering mules, such as being asked to transfer money they receive from an actor to various accounts he recommends. There are few publications on combating romance fraud using machine learning techniques. In the article Automatically dismantling online dating fraud,\textsuperscript{52} a system was presented that detects fraud or scams on dating sites with a high degree of accuracy, but there were many false-negative classifications in the results, as it turns out that real profiles have very similar characteristics to fake ones.


Ransomware

Ransomware is a form of malware that has the ability to encrypt a victim’s computer systems and digital information, prohibiting access until a ransom is paid to attackers. Malware is malicious software created with criminal intent to gain undetected access to the computer systems of its victims. There are various forms of malware, including Trojans, rootkits and viruses. The typical payment requested by criminals is in cryptocurrencies due to the anonymity surrounding wallet owners.

Ransomware is a sophisticated method used by financial cybercriminals. Its popularity is growing, as seen in recent attacks – the 2021 attack on Colonial Pipeline in the US, the Irish Health Service Executive and the highest-ever ransomware attack on the Acer company with a demand from cybercriminals to pay $50 million. Between 50 and 75 per cent of ransomware victims are small businesses. Ransomware is a combination of the previously discussed methods in financial cybercrime. It is a mixture of cryptocurrency money laundering and social engineering to break into and gain access to corporations, companies and institutions. Preventative measures in the fight against ransomware include improved cyber security for potential victims and reactive measures, such as those seen in Elliptic’s blog articles, where money can be tracked and criminal organisations identified.

Deepfakes and GPT-4

With the development of ML models to counter financial cybercrime, technology has advanced to make it easier for actors to commit crimes. Deepfakes and sophisticated chatbots, such as GPT-4, are able to spoof and manipulate employees at all organisational levels. In March (still GPT-2) 2019, the CEO of a UK-based energy company believed he was talking to his superior, the CEO of the parent company based in Germany. This was in fact a sophisticated deepfake model implemented to commit a crime using social engineering. This enabled the criminals to profit around €250,000. Deepfakes are not only audio manipulations but also visual ones. Deepfake programmes are able to create completely fictitious identities of people. Websites use a Generative Adversarial Network to create a ‘persona’ and even generate modified images of people without

55 This is a multimodal large language model created by OpenAI and the fourth in a numbered series of ‘GPT-n’ basic GPT models. Electronic source: https://en.wikipedia.org/wiki/GPT-4, accessed: 17.05.2023.
their consent. These images can also be used in online profiles that can impersonate real users of sites such as dating sites or social networks.

GPT is trained to predict the next word in a sentence and has shown that it can create human-like chunks of text, such as news articles. GPT has been used to create fake reviews for retailer sites such as Amazon. Fake reviews can deceive genuine customers and lead them to transact with illegal suppliers or manufacturers of low-quality goods, as well as damaging the review’s total score and the company’s competitive reputation. ‘Handwriting’ comments on vendor websites is a method known as crowdturfing and is considered an attack on online review systems.

**Challenges and directions**

Fighting financial cybercrime is not an easy task. Financial cybercriminals (actors) are sophisticated in their attack methods and cunning in their use of social engineering methods. Although research is moving forward, for cyber security professionals, it is a constant struggle for existence. Below are the challenges and potential future research areas to work on.

Creating practical and effective machine learning or deep learning techniques requires not only accuracy in predictions but also speed. Particularly in finance, customers expect transactions to be seamlessly delivered to the right audience. The ambition to implement real-world applications in this industry requires the ability to update the underlying datasets in response to new transactions in real time, without unnecessary delays.

The emergence of cryptocurrencies, coupled with the use of DarkNet and related IP masking tools such as VPNs, makes the task of identifying financial cybercriminals more difficult. Methods for detecting cryptocurrency-mixing accounts are key in the masking, cryptocurrency laundering phase. A key area of research for cryptocurrency laundering is the exit strategy used by criminals. To be able to swap cryptocurrency for a more favourable currency, there are a number of methods, including the use of DarkNet-derived marketplace providers that accept cryptocurrency transactions in exchange for other physical currency. Other methods include more commonly used exchanges such as Coinbase or DarkNet-derived exchange marketplaces such as Hydra for gift cards and vouchers that can be used to purchase physical goods. Hydra, a Russian marketplace on the DarkNet, received more than $1.4 billion worth of bitcoins in 2020. In exchange for bitcoin, users receive prepaid debit cards. Common to all methods is the movement of cryptocurrency from one wallet to another, thereby recording an identifiable transaction on the blockchain. Identifying these accounts/transactions is a step in the right direction in combating methods in exposing the activities of fraudsters. More detailed use of

---

group/graph-based anomaly detection is needed to address community structures in networks.

Creating algorithms to combat criminals who deliberately conceal their activities requires robustness. This robustness of the model can be identified and measured by its weaknesses. Another challenge in designing a method to prevent criminal activity is to keep it updated with criminal activity and sophisticated techniques. To address this, future research should include attacks that attempt to infiltrate the model in an effort to avoid detection by algorithms. Through testing, weaknesses can be identified and then addressed through further experimentation with the model or re-evaluation of the entire algorithm. The robustness of a model includes its ability to adapt to changes in data and changes in features. These are common in finance due to changes in economic trends, customer spending habits and the introduction of modern technology.

Due to the heterogeneous properties of cryptocurrencies, modelling them in graph form is a challenge. Ethereum and bitcoin have different blockchain structures, where Ethereum is able to incorporate contracts into its transactions, while bitcoin is a simpler transaction method, but there are still many ways to represent nodes and edges in the graph construction stage. These different forms of representation require the user to build a specific graph to capture the transaction information necessary to perform the final task, such as money laundering or perhaps analysing the liquidity of outstanding contracts on the network.

Methods for detecting financial fraud have to work with incomplete and uncertain data. As material truth labels are sought through manual review by analysts, an updated fraud model may be outdated due to the lag in real-time availability of rich incidental data. The challenge is for ML systems to adapt and make decisions based on incomplete data. For example, in a typical AML use case, not every observation and latent relationship is available at decision time. This makes the design and evaluation of algorithms challenging. Self-supervised methods have the potential to have a huge impact on the future of anti-financial cybercrime research. Self-service graph learning approaches can allow us to understand and predict events without bias. There is a potential use case through DeepMind’s traffic prediction adaptation, which uses advanced graph neural networks and transforms them for financial networks to identify malicious users.

**Summary**

Analysing the latest algorithms, models and techniques used to combat various aspects of financial cybercrime, it is clear that this is not a trivial task. The way in which behaviours are obfuscated, manipulated and masked creates a daunting task for researchers and engineers who must ensure the identification, detection and prevention of malicious, illegal activity. As seen in the literature, group anomaly detection, deep learning and graph theory are combined to identify networks of malicious actors.
within general user and customer groups. With large sums of money extracted from the financial system, there is a penalty paid by the public through increased fees and a lack of trust in their private information held by companies. It can be concluded that financial cybercrime affects our society on a sociological level, especially in the area of money laundering and tax evasion. The lack of consequences or retribution for criminal activity can disrupt and create discoordination in the public’s perception of the police.

References


45. Song X, et al., Conditional anomaly detection, *IEEE Transactions on Knowledge and Data Engineering* 2007, Vol. 19, No. 5.


49. Ustawa z 1 marca 2018 o przeciwdziałaniu praniu pieniężnym oraz finansowaniu terroryzmu (consolidated text, DzU, 2023, item 1124).
Keywords: artificial intelligence, threat detection, behavioural analysis, fraud prevention, phishing detection, malware detection, vulnerability management, incident response, threat detection, predictive analytics, security automation

Summary: Combating economic cybercrime with artificial intelligence could be an effective new approach. This is because artificial intelligence technologies can detect and respond to cyber threats in real time, identify patterns and anomalies in large data sets, and automate various security processes. The main ways in which artificial intelligence can be used to combat economic cybercrime are threat detection, behavioural analysis, fraud prevention, phishing and malware detection, vulnerability management, incident response and threat detection, predictive analytics, and security automation. It is important to note, however, that while artificial intelligence can significantly improve cyber security operations, it is not a standalone solution. It should be used in conjunction with other security measures, such as regular software updates, employee training and strong access controls, to create a robust defence against economic cybercrime.

DOI: 10.5604/01.3001.0053.9746
http://dx.doi.org/ 10.5604/01.3001.0053.9746

Palarbas clave: inteligencia artificial, detección de amenazas, análisis de comportamientos, prevención del fraude, detección de phishing, detección de malware, gestión de vulnerabilidades, respuesta a incidentes, detección de amenazas, análisis predictivo, automatización de la seguridad

Resumen: La lucha contra la ciberdelincuencia económica por medio de la inteligencia artificial podría ser un nuevo método eficaz. Las tecnologías basadas en la inteligencia artificial pueden detectar y responder a las ciberamenazas en tiempo real, identificar patrones y anomalías en grandes conjuntos de datos y automatizar diversos procesos de seguridad. Los métodos principales que pueden emplearse para combatir la ciberdelincuencia económica son la detección de amenazas, el análisis de comportamientos, la prevención del fraude, la detección de phishing y malware, la gestión de vulnerabilidades, la respuesta a incidentes y la detección de amenazas, el análisis predictivo o la automatización de la seguridad. Conviene señalar, sin embargo, que si bien la inteligencia artificial puede mejorar significativamente las operaciones de ciberseguridad, no es una solución autónoma. Ha de utilizarse junto con otras medidas de seguridad, como actualizaciones periódicas del software, formación de los empleados y controles de acceso estrictos, para crear una firme defensa contra la ciberdelincuencia económica.