Criminals Cash Flow Strategies in Financial Crime on the Example of Online and Offline Fraud

Sven Kuhlmann, University of Magdeburg, Germany
Ronny Merkel, University of Magdeburg, Germany
Jana Dittmann, University of Magdeburg, Germany
Barbara Colette Zitturi, University of Graz, Austria
Martin Griesbacher, University of Graz, Austria

The European Conference on Psychology & the Behavioral Sciences 2016
Official Conference Proceedings

Abstract
Monetary aspects are an important factor in many criminal offences, especially concerning financial crimes, online and offline fraud as well as drug trafficking. In the scope of this paper, the issue is illuminated from different perspectives, based on two qualitative interviews of 32 prisoners and 7 anti-fraud experts. Investigated factors include crime motives, modi operandi as well as money managing strategies (laundering, hiding, spending and re-investment). Results indicate that, apart from each prisoners story being individual, cash is king for most offenders and that in the majority of crimes organisational and human weaknesses are exploited rather than technical security systems. Modi operandi are often learned from personal prison, milieu or other peer contacts and refined after first successful try-outs, whereas exit conditions are barely defined. Money laundering, hiding, spending and re-investment strategies vary between criminals, but certain strategies are repeatedly applied. Anti-fraud experts often confirm the findings from the prison interviews, however also perceiving the topic from a slightly different perspective. The collected information is regarded as a very valuable source for the reliable semantic modelling of a crime field ontology in the future, potentially assisting forensic investigators in the scope of automated reasoning and explorative search capabilities.

Keywords: Financial Crime, Online Fraud, Offline Fraud, Cash Flow, Study, Interview, Prisoners, Anti-fraud Experts, Motivation, Cyber Crime

Introduction and Motivation

Money plays an important role in many crimes. It is often the motivation of an offender to commit a crime, constitutes various financial flows during the crime execution and is an important subject of investigation after the crime, e.g. in respect to its distribution, laundering, hiding, re-investment or spending. Several studies on organised crime exist, such as (Europol, 2016a), (Europol, 2016b), (Austrian Federal Criminal Police Office, 2016) and (Bässmann, 2016), which provide a broad overview and give actual trends on the issue. However, in practical police investigations and trials, the specific whereabouts of stolen money are often unknown (e.g. in case of hiding) or non-reversible (e.g. in case of spending or re-investment). Also, knowledge about specific attacker motives as well as means of expertise acquisition and grouping processes are often fuzzy. A few of these aspects are summarized and presented in the scope of this paper, which are acquired from 32 captive interviews in six German detention facilities. The interview study was developed and carried out to examine the issue from an inside perspective of the criminals. The paper does therefore not focus on statistical or quantitative analysis, but rather on intra-personal relations and related motivation, knowledge, tools and behaviour.

As cash flows become more and more digitized, the identification and analysis of computer-related crime gained significant importance. “Cybercrime” is one of the most commonly used terms to refer to this increasingly important field of policing (Wall, 2001), which not only includes fraud and forgery but also a wide area of other criminal activities (e.g. cyber trespassing, piracy or child pornography). To better understand the differences between the offender’s views on their own activities and the expert’s views on cyber crime, a second interview study was conducted with seven experts from the fields of criminal investigation, financial services and the IT-sector, concerning the issue of cyber crime (cyber deception and thefts, including fraudulent use of appropriated credit cards and cash). The different perspectives of both studies are visualized in figure 1.

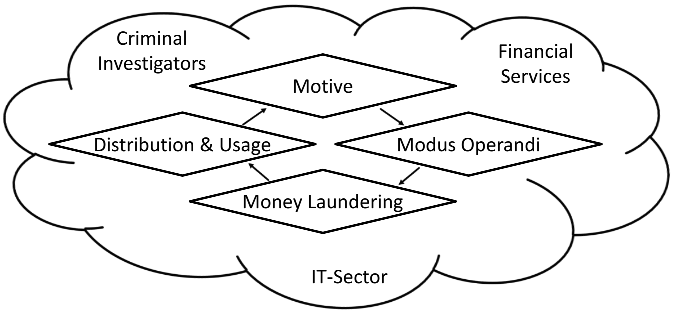

Figure 1: Different viewpoints of the conducted prisoners and anti-fraud experts interviews on financial aspects of online and offline fraud.

In respect to forensic investigations, experts have to structure case facts and identify links between them, to successfully solve crimes. In recent work (Merkel et al., 2016), a semi-automated, holistic framework has been proposed to combine information from the three domains of public knowledge, forensic expert experience as well as captive interviews into a financial crime field ontology, which might assist investigators to discover links between various crimes in the form of semantic reasoning and an explorative search. However, such approach relies heavily on the reliability and comprehensiveness of the modelled information. It is therefore of utmost important to collect modelled information from as many different viewpoints as possible, especially from the perspective of the criminals and other affected parties (e.g. anti-fraud experts), to assure that the created model will be of a certain reliability.

Method and Study Description

The study was realized in seven prisons in Germany. In total, 32 prisoners were interviewed. The interviews took between one and three hours in an advocate room and were audio recorded. The prisoners were preselected either by the criminological research institutes or by the staff of the prison. The selection criteria are online and offline fraud, crimes related to payment and credit cards as well as drug trafficking. The reason for these selecting criteria was to find interview candidates with crimes involving a high amount of money, its transfer from virtual money (e.g. bank account or Bitcoins) to cash and vice versa as well as money laundering. After selection, the candidates were invited to the interview and briefed beforehand as well as at the beginning of the interview about the voluntary nature and anonymisation of the provided information. The interview was structured based on a field manual containing social and crime related questions. The sequence was not fixed, leaving the possibility of narrative excurses.

The evaluation is based on a qualitative in depth analyses of the focus relevant interview data. The specific findings of potential motives, group organisation, contact acquisition, modi operandi, used knowledge and tools, money laundering and hiding strategies as well as spending and re-investment behaviour might be included into the crime field ontology of (Merkel et al., 2016) in the future, to complement knowledge obtained from expert experience and public domain information. Such ontology can potentially be used in the scope of forensic investigations to assist experts in the explorative discovery of links between specific case facts as well as to provide automated semantic reasoning. Based on this formal representation, inter-personal and inter-crime connections might be identified and compared to the reported motivation and risk estimation as well as the influence of know-how, tools and imprisonment.

Complementary to the interviews with the prisoners, the findings of a second study were assessed, comprising seven Austrian experts from the most important fields of cyber security: federal criminal investigation, financial services including banks and the IT-sector (programming of security and financial software). These interviews took between one and three hours and broached the issues of cyber crime, cyber security and mobile payment technologies.

The Role of Money in Motivation and Modus Operandi

Motives for committing online and offline fraud are usually related to the realization of profit. However, several reasons for requiring additional funds are provided by the criminals, ranging from covering living or health costs to financing different addictions (drugs, gambling, partying) or high living standards (partially resulting from earlier crimes). The results from the interviews show no significant correlation between the motivation, social background or modus operandi. Since all interviewed prisoners had several previous convictions – often for varying offences – only those offences relevant to the topics of this paper are reported in the following.

From an offenders perspective, the first offences are in many cases “try outs“. Typically, the motivation was supported by a (milieu) friend, relative or fellow inmate who reported the modus operandi to the offender. Sometimes, additional information was obtained over social contacts to experts and insiders as well as from documentaries, the internet or even seminars. After the successful completion of first offences and the related profit, the motivation often changes: the living standard is quickly adapted to the additional money, creating a substantial motivation for further crimes. A clear picture of a certain objective, e.g. a new car or to amortise a debt was seldom observed. In most cases, the motivation for profit from the offences was more diffuse and could be summarised as “would be nice to have”.

The initial living standards (before conducting financial crimes) varied from lower income (social welfare) to upper middle class (approx. 5000 Euro per month) and show no significant correlation. Criminal activities seem to be more related to the opportunity and the positive results of the first offences. Paired with the experience of success and missing arrestment, the interviewed offenders reported a high attraction for repetition. In the following, they adapted their living standard, which resulted in higher costs and a higher offence frequency.

A refinement of the modus operandi was often observed, motivated by an increase in profit or a decrease of risk, both of which play an important role. No offender changed the modus operandi completely – the type of crime was kept, often even after imprisonment. For example, in cases of drug trafficking, an adaption was sometimes reported by outsourcing the transport of drugs across the border or reducing the number of buyers. In other crime fields, modi operandi were changed according to additional security measures designed to prevent the exploitation of certain weaknesses. In case a new security feature prevents a modus operandi completely, the criminals often move to other countries, in which the vulnerability remains.

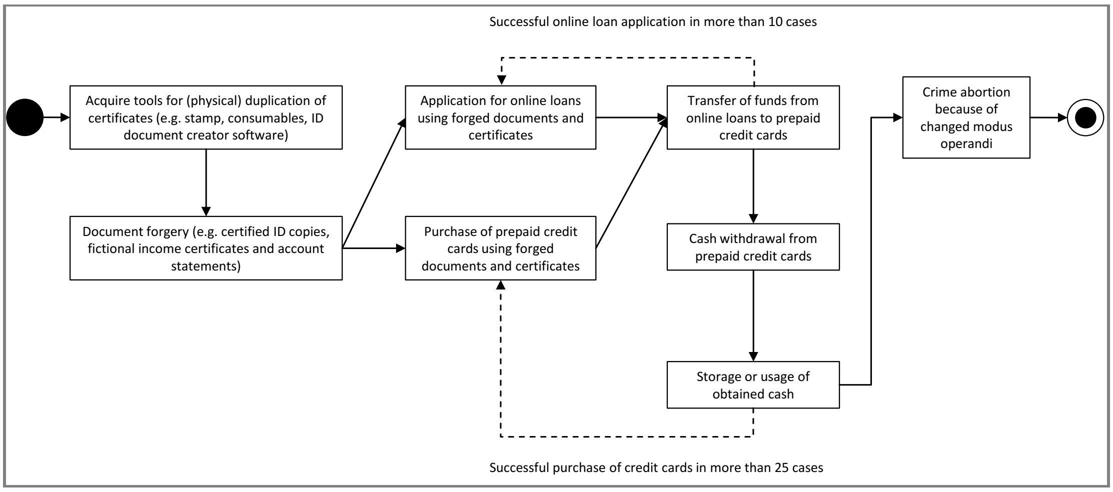
Successful online loan application in more than 10 cases
Acquire tools for (physical) duplication of certificates (e.g. stamp, consumables, ID document creator software)
Application for online loans using forged documents and certificates
Transfer of funds from online loans to prepaid credit cards
Crime abortion because of changed modus operandi
Document forgery (e.g. certified ID copies, fictional income certificates and account statements)
Purchase of prepaid credit cards using forged documents and certificates
Cash withdrawal from prepaid credit cards
Storage or usage of obtained cash
Successful purchase of credit cards in more than 25 cases

Figure 2: Initial modus operandi of an exemplary loan fraud case.

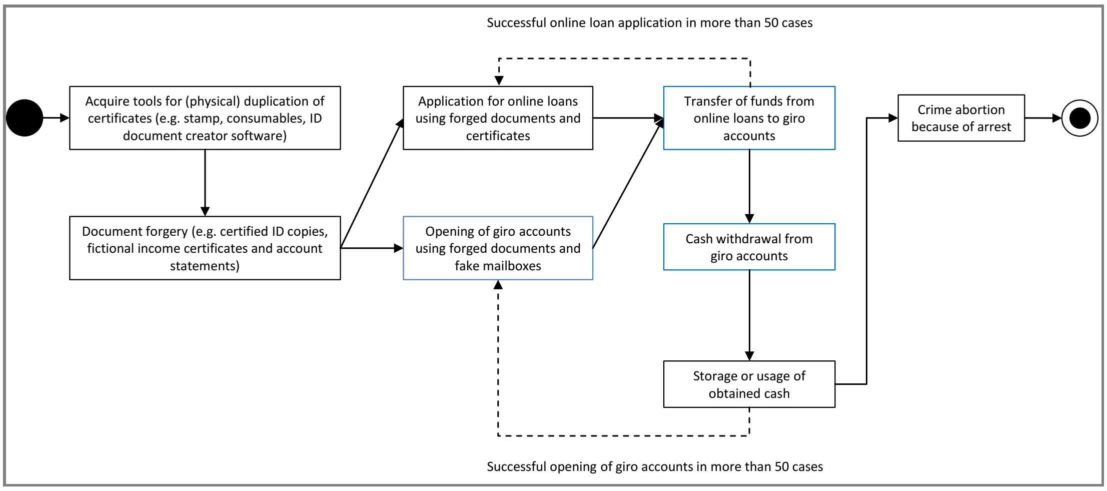
Successful online loan application in more than 50 cases
Acquire tools for (physical) duplication of certificates (e.g. stamp, consumables, ID document creator software)
Document forgery (e.g. certified ID copies, fictional income certificates and account statements)
Application for online loans using forged documents and certificates
Opening of giro accounts using forged documents and fake mailboxes
Transfer of funds from online loans to giro accounts
Cash withdrawal from giro accounts
Storage or usage of obtained cash
Crime abortion because of arrest
Successful opening of giro accounts in more than 50 cases

Figure 3: Refined modus operandi of the loan fraud case after security enhancements by the bank.

The modus operandi of an exemplary loan fraud case is introduced here, depicted schematically in figures 2 and 3. In the initial modus operandi (figure 2), the criminal acquired tools for creating duplicates of certified documents, such as ID creator software. With these tools, he forged certified copies of fake ID documents and salary certificates. he then exploited certain organisational weaknesses in the German Postident system, e.g. as described in the German news report of (Schader, 2015), to authenticate his false identities as legitimate German citizens. Using these faked identities and certificates, he was able to successfully apply for online loans, of which he transferred the received funds to purchased prepaid credit cards (which are comparatively easy to obtain, because they allow only to withdraw money which has previously been charged onto them). He then withdrew the money from the prepaid credit cards and stored or used the obtained cash. He successfully repeated this modus operandi for about ten times before he had to abort the crime due to changed security measures by the bank, which did not allow to transfer granted loans to prepaid credit cards any more.

Due to the increased security measures, the criminal changed his modus operandi (figure 3). While the creation of fake documents remained, the prepaid cards could no longer be used for withdrawing the loans. Therefore, the criminal opened fake bank accounts using the created false documents and the earlier introduced weaknesses. To receive the debit or credit cards from the bank, he installed fake mail boxes at remote locations, where he would pick up the documents and cards. The granted loans were then transferred to the created bank accounts and withdrawn using the corresponding cards. The criminal managed to repeat this modus operandi in more than 50 cases before he was arrested.

This exemplary offence confirms a general trend observed from the prison interviews: the tendency to target organisational or social weaknesses, circumventing technical security mechanisms. This would also mean in return that increased technical security measures (e.g. authentication measures replacing the Postident system) might be able to improve the resilience to these kind of attacks to a certain extent. As another important trend, criminals reported in most cases to not have clear conditions when to stop a certain modus operandi. Therefore, they often go on performing a certain crime until they eventually get arrested.

The Role of Money in Laundering, Distribution and Usage

In many cases, the offenders reported a high amount of profit, which led to different laundering, distribution and usage strategies. In general, there was a tendency towards transferring gained money into cash as quickly as possible and then dealing with cash only. Digital money, such as Bitcoins, was used in some cases, however mainly for purchasing data to be exploited (e.g. credit card data) or software tools (e.g. document creators), rather than for money laundering or hiding. When being asked about Darknet transactions, some criminals answered that they have not used this technique yet, however seemed to have thought about this topic for potential future use. However, the use of Bitcoins seems to be limited to certain types of criminals, such as cybercriminals or computer affine people. An interesting study concerning the acceptability and usage of Bitcoins amongst common people is given in (Krombholz et al., 2016).

Used money laundering strategies included gambling in casinos (considering the cash out as clean money), insurance fraud (e.g. buying cars and provoking accidents, receiving money from liability insurances of other motorists), buying real estates, cars and other goods with cash. Few criminals were hiding the money in bank deposit boxes, hideouts in their house or bank accounts (e.g. in other countries).

When a criminal is caught by the authorities, the whereabouts of the looted money are often unknown and can seldom be retrieved (Eisenberg, 2005). Convicts often report to have spend the money on gambling, parties or living. Also, the money is sometimes re-invested into new criminal activities (e.g. buying drugs or other resources for criminal activity). A typically used strategy is to buy houses, which are then transferred to relatives or trusted people and can therefore not be confiscated by the authorities. Sometimes, these people also help to transfer money to other countries. Private foundations might be used, preventing state authorities from gaining access to the money. Furthermore, it was also reported by the criminals that a more secure strategy to deposit money is by using a foreign bank account. In this case, the criminal selects a country that has a strong protection of bank customers and does not cooperate with authorities. Another strategy is the transfer of the money (in most cases cash) to trustworthy persons or relatives, which transfer the money to a bank deposit, hide it, take it out of the country or re-invest it (e.g. in a pawn shop). This strategy has two reported disadvantages: the first is the potential identification by the authorities and the related risk of losing the money and the second is the level of trustworthiness of those relatives or business partners, since there is always a certain chance of them disappearing with the money.

Almost all interviewed offenders reported to avoid transfers from cash to no-cash (e.g. bank accounts) because it may leave traces. Thus, cash plays an important role in financial crime, since it is the most reliable strategy to keep the money from being discovered. Especially in online fraud, a transfer from bank money to cash is therefore essential and was reported as a high risk situation.

In summary, money spending strategies also partially vary based on prior experience with imprisonment. If there is no prison experience or hints of imminent imprisonment, the money is often spent loosely for parties, goods or gambling. If there is prior prison experience or insight knowledge that they might get caught and imprisoned, the offenders often reported about different strategies of putting money aside. Since bank accounts implicate the risk of being detected and confiscated, the offenders tend to more reliable strategies: hide or dig as cash (risk of being found), give it to a third person that is not involved in the crime (risk of being detected by the police or of being betrayed) or the investment in real estates (risk of being detected). Whether such strategies are adopted by a criminal usually depends – apart from prior experience with imprisonment – on individual preferences and personality.

Anti-Fraud Expert's Views on Cyber Fraud, Cyber Offenders and Cyber Security Strategies

In addition to the offender's view on criminal activities and motivation, there is also the need to consider the opposite perspective. Experts on cyber fraud, cyber offenders and cyber security were interviewed in a second study, consisting of criminal investigators (3) representatives of the financial service sector (2), and IT-experts (2). The interviews provide further insight into the analysed problems of cyber crime. The expert interviews didn't focus directly on descriptions of cyber offenders, but covered cyber crime as a broader phenomenon. When talking about cyber crime, all experts tended to focus mainly on well organised criminal groups. In offender descriptions during the interviews, they seem to set the focus on uncaught and successful offenders.

According to the interviews with anti-fraud experts, the offenders main objective in the area of cyber fraud is seen in gaining money (other areas of cyber crime like piracy or hacking differ in this regard). The origin of offenders is often supposed to be in countries with a poor social system, poor living standards and high unemployment rates compared to industrialized countries. This seems to be seen as one reason to get into cyber crime. During the interviews, one motive has been assumed to be the (a) "need to survive", while others have been located in gaining (b) higher living standards and (c) more money. Furthermore, during the conducted interviews, financial service and IT-sector experts pointed out that some attacks may also be carried out of boredom or to simply see if it is possible to get away with a certain attack. In contrast, boredom was seldom reported as a motive in the prisoner interviews. However, this might be a particular motive for cyber crimes, but seems to be less common for crimes with a high offline component. Prisoner interviews have not only revealed offenders from poor countries, but also from Schengen countries, showing that online and offline fraud is not necessarily related to poor living conditions.

According to the interviews with anti-fraud experts, some offenders, especially the successful ones, are perceived as being well trained and educated persons in the field of IT-technology and are easily and quickly able to adapt to new circumstances as well as technological developments and changes. A lot of expert knowledge (state laws, IT-technology, company structures, social skills) is required to be able to use technological developments for criminal purposes in a creative way. Hence, expert interviews describe some offenders not only as being well trained and highly educated (especially in the IT sector), but also as socially skilled or intelligent, quickly able to built up on-the-spot-trust-relationships and to use changes in the complex modern world (e.g. information explosion, acceleration, change in temporal structures, expanding individualisation, loneliness and accompanying overextension) for their own good. In addition, prisoner interviews have also surfaced runners, money mules, drivers and simple computer fraudsters, which are often not very well educated or socially skilled. Therefore, also people with poor skill levels are included in online and offline fraud, but with a significantly increased probability of getting caught.

Some cyber criminals are described as being very well organised, structured and elaborated in their working behaviour by anti-fraud experts in the interviews. Offenders often seem to have built an organisation-like structure, if necessary, in which the work is based on a elaborated division of labour. The experts emphasized that the offenders work is – as long as located in the cyber space – geographically unbound and with free time management. In comparison to a working place with fixed working hours and timetable, these seem to be more convenient working conditions. To a certain extent, these advantages disappear when the modus operandi also includes offline components. The prison interviews have also shown a division of labour in different cases, but individuals have also been reported to commit crimes on their own, e.g. because they fear an increased chance of being detected through the mistakes of others. Additionally, for some modi operandi, a division of labour has not been necessary (e.g. loan fraud). In general, individual criminals seemed to be more willing to share information than the ones working in organised groups.

The possibility to be anonymous and faceless in cyber space is another characteristic of cyber fraud seen as beneficial for the offender. Interviewed prisoners were also pointing out this benefit of an increased anonymity when using online means, e.g. the Darknet for trading data and tools.

As reported by the anti-fraud experts, the transition of virtual money gained in online fraud to real (bank or cash) money is an important aspect, because the used interface might allow finding traces potentially leading back to the offender. For the interviewed criminals, it was of great importance to quickly transform the gained money into cash, which is much easier to split, launder and hide. Therefore, the cashing out of gained funds might be an interesting aspect for forensic investigations. The offline components of the modus operandi in cyber crimes are also very important, because for anti-fraud experts it's often hard to acquire traces of criminal online activities on the computers of victims, who often don’t allow access to their hardware.

All interviewed experts seem to agree that additional security measures are necessary, from building highly secure technical products to the education and information of companies and citizen, which all seem to be key elements to prevent cyber fraud and increase cyber security. However, the prisoner interviews have shown that if modi operandi are not working anymore (and cannot easily be adapted) due to the increase of security mechanisms, criminals often move on to other countries, which are still lacking these mechanisms. This country movement was also pointed out in the interviews with anti-fraud experts. Strengthening common sense interaction with IT-products and getting used to fast changing technical developments can therefore be seen as an important measure for a more comprehensive crime prevention, especially when spread internationally.

Conclusion, Limitations and Future Work

In this paper, **two studies** on monetary aspects of online and offline fraud were presented, showing first qualitative results of the views of involved criminals (32 subjects) and anti-fraud experts (7 subjects). Especially when interviewing prisoners, it can be concluded that personal stories leading to certain crimes are often very individual. However, the applied methods and modi operandi follow similar patterns in most cases. Monetary gain is often the main motivation for committing crimes, either to survive, keep high living standards or just to try out new ways to make money, quickly followed by new crimes to keep the achieved living standard. Offenders were of differing financial background (very poor vs. comparatively high salaries), differing countries of origin (poor countries vs. Schengen countries) and worked in organised form as well as alone. Modi operandi were mainly acquired from milieu, prison and family or friend contacts, but also from documentaries, internet and seminars. They were successively refined according to expanded knowledge, labour division strategies or additional security measures by the victims.

Money was usually transferred into cash as quickly as possible and then spent for gambling, parties or drugs. More sustainable money managing strategies included re-investment in future crimes, the purchase of goods (e.g. cars) or real estates, physical hideouts and transfers in the form of cash, goods or real estates to uninvolved, trusted people (to avoid confiscation). Money was in a few cases hidden in Bitcoins or anonymous accounts in foreign countries (such as Austria or Malta). Typical laundering strategies included casinos, cash purchase of cars, houses and other goods, insurance fraud, delivery returns and prepaid cards. Transferring cash to bank money was avoided. When a criminal is captured, the looted money can usually not be retrieved.

The study showed that in many cases the weakest points are not the pure technical implementation or securing mechanisms. In nearly all cases the criminals identified organisational or process-related weaknesses or procedures where humans are involved and can be outwitted. From this perspective, especially the implementation and security of processes beside the technical prevention should be further evaluated and improved.

Anti-fraud experts seem to have a comparatively realistic view on these reported strategies, but seem to vary in some aspects regarding ascribed expertise, motive and origin of offenders. However, this might be attributed to a slightly different perspective. The experts were often confronted with petty criminals as well as well-organised criminal groups. It seems that, during the conducted interviews, they tend to focus more on uncaught offenders, which are not located in their own national context. This is also related to international differences especially in the financial services infrastructure. While governmental anti-fraud agencies try to identify weak spots in the modus operandi of cyber crime offenders, service provider often focus more on the potential financial damage caused by trust issues. Financial service providers are engaged in strengthening their computer security as well as the acceptance and trust of their services and products. In the domain of cyber security, catching offenders seems to be only one of several policies fighting cyber crime. However, an empirically based analysis of the modus operandi of cyber crime weak spots – like the link between online and offline criminal activities – could improve counter measures and therefore strengthen cyber security.

Limitations of the studies can be seen in their qualitative nature, not achieving statistical significance of the results. Furthermore, in psychological studies, there is always a certain error, loss and uncertainty, which might be even greater than in the field of computer forensics, from where these measures are derived (Casey, 2002). Errors might easily occur due to different language conversions, e.g. using fellow inmates as translators and even when using professional translators. Furthermore, information obtained from interviews is trivially not complete and valuable information might be lost due to an incomplete amount and direction of questions asked. Uncertainty (or fuzziness) is another important factor when human communication is concerned, because language is derived from thinking in a certain (so far unknown) way and transferred through different channels (e.g. verbal, non-verbal, para-verbal) to the communication partners. Using such communication paths is subject to the widely discussed challenges of the linkage between thinking and language, the objectivity of communicated thoughts, psychological sender-receiver models as well as different language models. As a conclusion, the presented results can always be considered as subjective interpretations of the interviewers, even if a maximum neutrality was aimed at.

Future work should include a higher amount of interview partners for more reliable and quantitative results, allowing numerical statistical analysis strategies, e.g. cluster analysis. Within that method, a general and interactive connection between motivation, modi operandi and personal or financial background can be computed to derive and predict future criminal developments. Also, the crime fields might be defined more specifically to discover crime type related differences. The findings should be checked against publicly available information and statistics and should be modelled in a formal way, e.g. as proposed by Merkel et al. using a financial crime field ontology and logical reasoning (Merkel et al., 2016). They should furthermore be visualized in an efficient and scalable way to provide forensic investigators with better and semi-automated means for evidence structuring and crime investigation. Furthermore, emerging trends and corresponding preventive measures should be extracted and discussed from the findings of the studies.

Acknowledgements

The work in this paper has been funded in part by the German Federal Ministry of Education and Research (BMBF), funding code 13N13473. The expert interviews were conducted in a project ("3B3M") funded by the Austrian Research Promotion Agency (FFG) in the KIRAS Security Research Programme. We also thank Christian Kraetzer for his support.

References

Austrian Federal Criminal Police Office (2016). Cybercrime 2014, available at: http://www.bmi.gv.at/cms/BK/publikationen/Cybercrime.aspx (06.06.2016).

Bässmann, J. - German Federal Criminal Police Office (2016). Täter im Bereich Cybercrime - Eine Literaturanalyse, available at: http://www.bka.de/nn_258772/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/SonstigeVeroeffentlichungen/2015TaeterImBereichCybercrime.html (06.06.2016).

Casey, E. (2002). Error, Uncertainty and Loss in Digital Evidence. In: International Journal of Digital Evidence, vol. 1(2), pp. 1-45.

Eisenberg, U. (2005). Kriminologie (6). München: Beck.

Europol (2016a). The Internet Organised Crime Threat Assessment (IOCTA) 2015, available at: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015 (06.06.2016).

Europol (2016b). Exploring Tomorrows Organized Crime, available at: https://www.europol.europa.eu/sites/default/files/edi/EuropolReportDigitalKeyTrends.html# (06.06.2016).

Krombholz, K., Judmayer, A., Gusenbauer, M., Weippl, E. R. (2016). Für bare Münze? NutzerInnenerfahrungen mit Sicherheit und Datenschutz bei Bitcoin. In: Meier, M., Reinhardt, D., Wendzel, S. (Hrsg.): Sicherheit 2016: Sicherheit, Schutz und Zuverlässigkeit - Beiträge der 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), pp. 137-148, Bonn, Germany.

Merkel, R., Kraetzer, C., Hildebrandt, M., Kiltz, S., Kuhlmann, S., Dittmann, J. (2016). A Semantic Framework for a better Understanding, Investigation and Prevention of Organized Financial Crime. In: Meier, M., Reinhardt, D., Wendzel, S. (ed.): Sicherheit 2016: Sicherheit, Schutz und Zuverlässigkeit - Beiträge der 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), pp.55-66, Bonn, Germany.

Schader, P. (2015). Sicherheitsmängel bei Postident: Eintrittskarte für den organisierten Betrug, available at: https://krautreporter.de/711--sicherheitsmangel-bei-postident-eintrittskarte-fur-den-organisierten-betrug (11.07.2016).

Wall, D. (2002). Cybercrimes and the Internet. In: Wall, D. (Ed.): Crime and the Internet, pp. 1-17, London and New York: Routledge.

Contact email: merkel@ovgu.de