European Journal on Criminal Policy and Research
https://doi.org/10.1007/s10610-020-09438-3

ORIGINAL PAPER

Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms

Quentin Rossy[1] · Olivier Ribaux[1]

Published online: 29 February 2020

Abstract
A significant, and likely dominant, proportion of fraud is now conducted online. Police struggle to integrate this emerging reality into their processes, while expectations of this institution are high. These types of cybercrimes alter the volume and complexity of problems compared to how they previously manifested and require profound transformations of crime analysis methods to address them proactively. These developments face many difficulties, such as the quality of accessible data, the lack of existing analytical models and the need to increase police knowledge of fraud mechanisms within every level of organisations. We suggest methods to overcome these obstacles, which consist of implementing an approach integrating theories from various fields in criminology and forensic intelligence to examine the digital transformations of certain criminal processes. We take, as an example, how a generic script expressing the anatomy of an existing type of fraud can be used to interpret their new digital forms. This modelling activity both provides new insight into specific frauds and highlights relevant dimensions that are useful in orienting the development of crime analysis systems.

Keywords Online fraud · Confidence game · Forensic intelligence · Script analysis · Digital transformations

Introduction

Whatever uncertainties are associated with results derived from nascent methodologies, the existence of a large-scale, but ill-defined, computer-related crime problem is now evident (Goodman 2015; BCS 2016; Dupont 2017; Reep-van den Bergh and Junger 2018; BCS 2019). The emersion of a broad, multifaceted and unclear category of ‘volume cybercrimes and

✉ Quentin Rossy
quentin.rossy@unil.ch

[1] Ecole des Sciences Criminelles, University of Lausanne, Lausanne, Switzerland

frauds' requiring new forms of response had long been suspected (Button et al. 2014) and early attempts to characterise (Wall 2010), decompose and measure it (Smyth and Carleton 2011) were conducted. In this analysis, the broad category of online fraud, even if difficult to quantify, is admitted to contribute to a significant part of these crimes in Europe (Reep-van den Bergh and Junger 2018; BCS 2019). Fraud is an act of deception aimed at depriving victims of their money, data or other property. Online fraud must be understood as a type of fraud that benefits from the internet. Typical frauds occur in disparate social and professional activities, such as online shopping, when using online banking systems and Internet dating sites, or by intrusion, sometimes in the workplace, through e-mails using false qualities, identities and made-up stories. These crimes affect a proportionally largely victimised population (ABS 2016; Reep-van den Bergh and Junger 2018; BCS 2019) and their novelty constitutes a challenge in terms of public safety and police support. Police must offensively develop more new approaches to integrate this reality into their processes (Loveday 2018).

We wish to initiate a debate on how to consider the analysis and monitoring of online frauds in a police environment, mostly at an operational level. Indeed, within the police, many insightful investigators have warned of early signs of profound changes, although they have been largely confined to specialised and pioneering technical units, long marginalised within their own organisations (Burns et al. 2004; Pollitt 2010). The emerging response has primarily been limited to specific areas (Cross and Blackshaw 2015), generally the most serious and sophisticated forms of computer-related crimes, while the online fraud is pervasive and largely transcends police organisations (Loveday 2018).

Whatever these hesitations regarding what direction to take, the police should now offensively find their place (Cross and Blackshaw 2015; Levi et al. 2017; Loveday 2018). At a minimum, police must be considered a credible interlocutor when interacting with the public and other professional stakeholders regarding online frauds. They are tasked with recognising these modern forms of criminality in specific situations, knowing the content of their own data and structuring their treatment, from the first contact with the victim to more central analysis allowing for proactivity. They should design and suggest appropriate responses and advice, in terms of intervention, investigation and prevention. In other words, the development of new crime analysis processes that go beyond the treatment of traditional, high-volume crime is under question.

Initiatives exist upon which the police can build. Innovative cyber reporting infrastructures have been made available to the public, such as Action Fraud in the UK (Levi et al. 2017). Europol indexes around 20 such websites for European countries, allowing citizens to report their cases and enriching the available data.[1] Such a service, however, reveals many limitations and generates unrealistic expectations (Cross 2018). These platforms are, furthermore, generally not operated by the police, resulting in the increased fragmentation of relevant data.

In the first section of this paper, we focus on the problems police face in adequately recognising this online fraud, with specific cases. This helps to express gaps in the formalisation of these types of fraud and the lack of a harmonised framework, as well as of a general culture in the police. This makes obvious that the development of a well-expressed crime analysis model covering online fraud requires an interdisciplinary approach. To that end, we primarily focus here on certain types of fraud and their expansion online. Numerous examples of different kinds will be presented.

[1] https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

Modelling online fraud naturally leads, in criminology, to opportunities theories. These have successfully constituted a solid basis for the analysis of traditional, high-volume crimes (Clarke and Eck 2005). However, the extent to which these theories encompass online fraud is not straightforward (Yar 2005; Pratt et al. 2010; Leukfeldt and Yar 2016). The first challenge with the use of routine activity theories in our context is to define the virtual environments in which online fraud occurs. The scripts developed by Schank and Abelson (1977), popularised in criminology by Cornish (1994), advance this purpose. They support the decomposition of the activity in sequences to identify poorly protected environments in which the perpetrator gradually deceives the victim.

A generic script extracted from the so-called traditional confidence game, which has survived through the ages, serves as a first building block. This script allows the analysis of the anatomy of a wide variety of such frauds and their current digital transformations.

The scrutiny of interactions, virtual or otherwise, that occurs alongside these types of fraud then requires the consideration of psychological elements, specifically how cognitive biases, whose natures vary across time and certain populations, are exacerbated by perpetrators (Lea et al. 2009).

By expressing scripts and psychological dimensions, the nature and mechanisms of this family of online frauds are clarified. At the same time, these types of formalisation provide a framework for orienting the development of a crime analysis system. The model is completed by considering the elementary data that help to reconstruct and recognise the modus operandi and create links between incidents a priori separated. This entails considering the trace (digital or physical) constituting the vestiges of criminal activities. Recognising, collecting and deciphering information conveyed by the trace to support crime analysis belong to the field of forensic intelligence (Ribaux et al. 2016).

We suggest here the construction of an ambitious, global vision for the analysis of online fraud in a police environment. We demonstrate, however, that framed by the global vision, a more modest and realistic bottom-up approach is adequate to concretely implement elementary components, learn from situations, connect to other stakeholders and provide intelligence to proactively address the detected problems.

The Problem to Recognise

A key goal of devising a crime analysis system is to collect and organise data, to *recognise* already known forms of online frauds. Current processes and most existing classification systems are inadequate for this purpose.

At the highest analytic level, new indicators are introduced into official statistics to distinguish online fraud from other forms of crime. Typically, however, online fraud does not belong to offences that comprise the core of the statistical system. In some countries, a financial crime committed through the internet and reported to the authorities is still likely to be recorded as a physical property crime, not as a digital crime (ICPC 2018). Frameworks designed to host police statistics are basically unsuitable for grasping online frauds. Digital transformations add complexity and challenge the consistency of the model (Holt and Bossler 2016).

The harmonisation of new classification systems and surveys to allow for better statistical consideration is generally a stated goal, but this is difficult to achieve, and even more so at the international level (Reep-van den Bergh and Junger 2018; Caneppele and Aebi 2019).

Europol has taken the lead, at a more operational level, in Europe by defining a harmonised taxonomy of cybercrimes (EC3 2017). Such taxonomy could provide a starting point for filtering and sorting reported cases. However, such treatment of police data is strongly influenced by the perspective of law enforcement: the structure of the law has never been a good guide for the analysis of crime (Goldstein 1990). We discuss alternative proposals emerging from the criminology literature.

This problem of recognising online frauds is, however, not only related to the existence of a classification system. It is also a question of how field officers dealing with specific cases can themselves recognise the signs of online fraud. For example, in a specific region of Switzerland, a systematic review of reported cases was conducted; it found that in the data collected by the police via their reporting system, the amount of online fraud progressively increased to the same order of magnitude as domestic burglaries, generally without being correctly coded at the time of first registration. It was estimated that, for a population of nearly 800,000 inhabitants, 1021 frauds and 2871 domestic burglaries were reported in 2018 (Chinelli 2019). According to surveys (Reep-van den Bergh and Junger 2018), this value still lies well below the reality of the phenomenon (the online fraud reporting rate is estimated at between 10 to 15%). This number of cases available for analysis was already considerable. This was an excellent demonstration to show the police that they should be more aware of the data they already have.

Beyond an elite dealing with serious cases, some police organisations have created new structures at all levels by acknowledging the pervasiveness of online fraud. In Switzerland, criminal analysis and 'digital' services have recently and rapidly developed to become as important as traditional forensic services.[2] In this federalist country, such movement initiates, at the other end, bottom-up and more local approaches (Ribaux 2019). Field agents are now trained to recognise some of the new types of fraud by following a simplified, pre-defined list.

This is arguably a good starting point for initiating a virtuous circle: better recognition leads to better encoding, which creates better conditions for analysis. The production of intelligence and communication with the public will improve as well, and this leads to better public awareness and increased reporting rates. For the police, clearly expressing some dimensions of the problem will facilitate the definition of priorities and the design of a response.

This movement, however, is far from reaching its goal. Huge divergences between how different police organisations treat the problem highlight a further gap. In 2019, the various Swiss police (canton's police) published their official statistics separately through their own annual press conferences.[3] One canton reported a 131% increase in these 'volume cybercrimes', while another announced an increase of only 4% within the same framework of the national statistic model. In these two extreme situations, it is difficult to identify what the influence of management or the new activity of digital structures has been, or how the data were classified and encoded (and by whom), how the reporting rate increased or how much the problems themselves have evolved.

The problem of recognising online fraud hence remains far from solved. Fraud is often not even detected by the victims. It sometimes goes unnoticed, unrecognised or accepted as such. As an investigator acknowledged in a simplified manner, during an informal meeting, most often, 'the filing of a complaint remains essentially a meeting between a person [the victim]

[2] Polices cantonales, personal communications

[3] https://www.rts.ch/play/tv/19h30/video/selon-patrick-ghion-de-la-police-genevoise%2D%2Dune-des-grosses-erreurs-cest-de-faire-confiance-aux-messages-que-lon-reoit-?id=1031735525

who does not understand what has actually happened and a person [the police officer] who does not understand what happened to the victim'.

Although many current initiatives are converging towards a real trend in considering this new reality, the overall goal of developing a dynamic crime analysis system to detect new frauds and recognise relevant situations at all levels therefore remains far from being achieved.

In Search of a Crime Analysis Model

A systematic online fraud-monitoring project requires conceptualisation based on existing knowledge. How to distinguish different types of online fraud has been the subject of many proposals, based on various dimensions. Fraud is sometimes classified according to the means of communication used by the perpetrators (e.g. online, email, telephone), the targeting strategy (e.g. mass marketing fraud, targeted fraud), the type of victim (e.g. fraud against the state, businesses, individuals, persons with a particular profile), the type of asset sought (e.g. financial fraud, bank data theft, identity theft) or the kind of transaction (e.g. money transfer) (Button et al. 2009; Fischer et al. 2013; Button et al. 2014; Beals et al. 2015; Correia 2019: 3). Some typologies incorporate several dimensions into a single system, such as Wall's (2007) classification, which distinguishes between target fraud type, asset transfer methods and virtual space types. This variety demonstrates the complexity of the new area that must be covered. The relevance of these proposals for designing a comprehensive crime analysis system, however, remains difficult to discern.

Environmental and routine activity theories have facilitated an impressive integration of existing approaches into the analysis of traditional, high-volume crimes, which took years to develop (Clarke and Eck 2005). These theories thus constitute a very promising starting point to address our problem. However, some obstacles must be overcome to determine more precisely the aspects of the new crimes that can be covered by these theories, as well as where exactly the patterns lie upon which the response should focus (Yar 2005; Pratt et al. 2010; Leukfeldt and Yar 2016). A more complex aspect compared to the previous situation is the difficulty of defining the concentrations of activities in virtual spaces and, if necessary, linking them to physical spaces (Leukfeldt et al. 2017). The sale of stolen goods (which has a physical reality) through auction sites has both virtual and physical components that are difficult to express in a unique theoretical framework based on opportunities.

The famous routine activity saying 'meeting between a suitable target and a motivated offender in the absence of a capable guardian' (Cohen and Felson 1979) is not immediately expressed in virtual spaces. How people meet in social environments designed by email, social networks or websites changes considerably from how they interact at a specific location at a particular time. To understand new mechanisms related to routine activities, the study of digitally transformed meeting environments is of paramount importance.

However, this is not enough. A single fraud can involve several operations and types of meetings during its deployment. For example, identity theft, hacking and phishing often constitute full categories in classification systems, whereas they in fact enable other types of fraud (Holt and Graves 2007; Levi 2008; Whitty 2015b). The modus operandi developed by fraudsters who deceive their victims requires a series of steps that suggest the integration of various illicit activities or services into a whole crime system. These are generally difficult to detect and reconstruct with the accessible data. A *relative or friend imposter* scam involving a request for support aptly illustrates such an entanglement of activities.

Case study: Relative or friend imposter scam involving a request for support
By sending emails to plead for help, fraudsters adopt the identity of false acquaintance of victims to ask them for money. For this, the author exploits the pretext of an emergency: during a trip abroad, he has lost his money and travel documents. He then convinces the victim to transfer money through an international transfer service. To commit such fraud, the perpetrator must first know who a credible acquaintance (e.g. a friend, a relative or a colleague) of the victim could be, and under what 'mask' (e.g. an email address) he must present himself. This is done, for example, by accessing victims' email accounts and stealing all the email addresses from their lists of contacts. The author can then send the fraudulent message to these recipients, pretending to be the person. In turn, this access is obtained by stealing credentials from victims' mailboxes (or social media) accounts. This can be achieved by various means, for example, by hacking computers with malware or by phishing. Mobile phone hacking also allows fraudsters to gain access to a list of potential victims via instant messaging.

In this example, the entire mechanism includes a chain of activities individually recognised as offences, such as phishing and hacking, leading to identity theft. Links between these individual steps are difficult to establish, even if one or several elements of the chain has been detected, for instance, by the police. Downstream of the fraud, money laundering activities can occur. Money mules transfer the gains of the scam through their personal accounts. In other cases, goods purchased with stolen data transit through package mules. If each case is considered individually, the chances of reconstructing the overall system are minimal.

The separation of activities in a chain of operations also leads to some form of division of criminal labour. The Internet has reconfigured interactions between criminals, who can meet virtually in online convergence environments, such as forums, where they share, exchange and sell their services (Soudijn and Zegers 2012; Sood and Enbody 2013; Leukfeldt et al. 2017). For example, hackers possess the technical skills to steal data and sell them to fraudsters who can monetise them (i.e. transform data into money) (Dupont 2013). Finally, other types of participants transfer assets and launder financial products. Such a succession of steps usually occurs in the consumer fraud model called triangulation, in which the scammer sells, at a reduced price, a product he has purchased from a legitimate site with stolen credit card data (Gregg and Scott 2008). Victims can also become accomplices, when the fraudster publishes a job offer and recruits people for smuggling activities, for a commission.

Hence, crime analysis must consider that frauds consist of a series of intertwined activities that can be perpetrated by separate groups of criminals with sometimes weak ties to each other. It is necessary to formalise such sequences for analysis purposes. For example, Levi (2008) suggests using scripts for fraud networks, Whitty (2015a) for romance fraud, and Choi et al. (2017) to describe telephone fraud. Such script-based approaches can be generalised.

Confidence Games as a Script

Embracing the entire spectrum of fraud types with a single model seems intractable with current knowledge. We suggest adding a new component to the set of existing scripts describing fraud families, focusing on a specific form which we claim contains certain genericity. Our choice is also guided by our objective of using scripts to provide a formal

basis to help decipher how the old variants of certain frauds have been transformed by digitisation.

It is indeed surprising to observe how some deception mechanisms remained stable over time, well before digitalisation. Some very old tricks are still used today. This is true for a wide range of frauds that have been gathered in the category of *confidence game*. These are assumed to underlie generic mechanisms present today in a significant variety of online frauds. With the support of such a framework, the analysis of digital transformations and online versions of these frauds will be simplified. The aim is to obtain basic indications about the size of the changes and directions to be taken for the development of a crime analysis system. Confidence games, which possess a certain degree of genericity, thus serve here as a building block in the perspective of constructing a more ambitious framework covering a wider range of online fraud.

The term 'confidence game' was coined based on a specific event reported in a New York newspaper. On 7 July 1849, in New York, a man named Thompson was arrested. His modus operandi was to convince a chosen person in the street that he was an old acquaintance. 'He would say, after some little conversation, "have you confidence in me to trust me with your watch until tomorrow"' (New York Herald of July 8, 1849, cited in [Bergmann 1969: 561]). Of course, the man and the watch never reappeared. The confidence man (or con man, con artist) has become an important concept for discussing broader societal problems. At that time, forms of incentives considered comparable to confidence games had been used to trigger investment from modest people around the development of finance on Wall Street (Schur 1957; Bergmann 1969; Halttunen 1982). Even if the technique of the con man was not new (Halttunen 1982), the notion has gradually become common knowledge since that period.

The type described by Maurer in his seminal book, first published in 1940 (Maurer 1999), falls under the category of motivating the victim to invest in an equivocal enterprise. To this end, the con man plays subtly with the desires, beliefs and preconceptions intrinsic to the human mind. The sulphurous nature of the scenario, as well as, in a second stage, dishonour or humiliation, deters victims from reporting cases to the police. This reduces the risk for the perpetrators.

The search for an appropriate 'mark' (a person with a promising profile, depending on the scenario of the game) and the creation of a climate of trust that encourages the 'mark' to engage in the scenario is at the heart of the modus operandi.

Such frauds have been identified in Europe as 'American-style theft'. The various modi operandi were detected and described in detail by researchers and police officers interested in this phenomenon (Canler 1882: 206–217; Reiss 1911: 287–292; Louwage 1932: 88–94). Common characteristics were that the mark did not reside where the game was played, had good reason to carry money or showed signs of wealth.

Thompson's modus operandi was simple and consisted of questioning the victim on the issue of trust. Other confidence games are more complex and rely on constructing trust situations (Braucher and Orbach, 2015). According to Maurer (Maurer 1999), short cons target the money immediately available from the chosen mark and are generally limited in duration. Big cons are more elaborate, require staging and occasionally the use of stores and several specialised actors to gain confidence and allow victims to access their bank accounts and savings.

There is no doubt that short cons continue to flourish in the physical world in many forms (the old acquaintance trick is one, among many others), while big cons have expanded and transformed through the Internet.

Inspired by Maurer (1999), a simplified generic script emerges that describes the overall mechanisms of the modus operandi:

1. Search and contact potential marks
2. Reinforce the credibility of the scenario and establish trust
3. Trigger delivery of the asset
4. Take distance with the mark
5. Make use of the asset

The rich Spanish prisoner (a very old confidence trick), which belongs to this family of advance fee frauds that continues to flourish under many forms, follows this script. From the Middle Ages, similar scenarios later appeared, as in the letters from Jerusalem described by Vidocq at the end of the eighteenth century (Vidocq 1853: 58).

1. A supposed Spanish prisoner sent letters to request assistance. An example of such a letter, dated from 1898, was published in 1949 (D.H.H. 1949: 265):

> Prisoner since some time ago by sustaining free ideas of republicanism, I had the misfortune of to be persecuted by my merciless enemies of politic life, by whose consequence I was obliged to go out of Spain carrying with myself an important sum, which I had the necessity to hid into a sure place of your neighbourhood. Could you to give me your aid pecuniary for to recover it? I sure to you that perhaps this should contribute very much to enlarge the limits of your own prosperity, if well now is impossible for me to give you more particulars referent to this matter, but if you will answer this letter, I shall be pleased in manifesting to your openly what now I cannot.

2. The proposed scenario was designed to encourage recipients to respond to the letter. The deception is a false promise of an important commission. Once marks have announced themselves, it is a matter of creating a contact in a way of reinforcing the credibility of the game and, generally, acquiring the trust of the mark.
3. Under many pretexts (obtaining an official document or paying a tax, a suitcase left on deposit, a bribe, etc.), the perpetrators repetitively claim fees of relatively small amounts compared to the expected gain. It is important that the next payment gives the mark the feeling of moving forward towards obtaining the promised gain.
4. Stop sufficiently early the process to minimise risks. Ensure that the mark, once aware of the scam, is unable to identify and locate the perpetrator.
5. Make use of the money.

This generic script is an initial description that allows one to distinguish primary activities at a general level. An entire script structure is a hierarchical structure where nodes (each representing a script) are linked by a genericity/specificity relationship (Schank and Abelson 1977). This means that it can be specialised further based on in-depth knowledge in specific areas. For example, Whitty (2015a) proposes such a description for a specific advance fee fraud called a romance scam (i.e. proposing attractive fake profiles on web-dating sites).

Digital Transformations Interpreted Through the Script

Routine activities now occur in digitalised environments (i.e. environments populated by electronic devices) that generate a new volume and variety of data. These are treated with varied social and economic objectives on a time scale that has changed considerably (Laney 2001; Günther et al. 2017). These new spaces alter opportunities for social interactions and change their nature. They challenge moral values (e.g. privacy), incorporate new business models and provide explicit value to the data that are craved by fraudsters (e.g. personal data, a gift card code).

This changing landscape has exerted a major impact on fraud. Computerisation and the internet are hence now intensively involved in fraud, but to varying degrees: from virtually no involvement (e.g. false police officer fining a tourist in the street) to an entirely computerised process (e.g. massive numbers of phone calls inciting calling back to a premium number). The roles of human actors in the fraud then also vary from physical encounters (e.g. exchange of a suitcase full of money with a suitcase filled with worthless paper—so-called rip-deal fraud) to the extensive use of new social engineering techniques enabled by information and communication technologies (Atkins and Huang 2013). McGuire and Dowling (2013) distinguish cyber-enabled crimes from cyber-dependent crimes (i.e. crimes that would not be possible without the internet). The possibilities to combine new techniques and adapt the degree of use of the internet and computerisation in a single fraud exponentially increase the number of possibilities without necessarily requiring extensive technical knowledge.

The script described in the previous section supports the analysis of these digital transformations and opens them for further specification at another level of granularity: how the frauds have evolved and their complexity has increased, how they are globalising, how their number has changed in scale, and what actually is new in some specific areas. We concentrate primarily on the mechanism of the fraud itself, with a particular focus on how fraudsters exacerbate cognitive biases that are particularly prevalent in certain populations and specific contexts. It should be noted that frauds are sometimes associated with upstream data theft activities. The use of the money (i.e. money laundering) is also only briefly described here.

Search for and Reach Potential Marks

The techniques for selecting promising marks have of course expanded due to information and communication technologies. With regard to advance fee frauds and the so-called Nigerian developments in the 1980s (Durkin and Brinkman 2009), letters were mailed for many years, sometimes using false stamps, probably to allow mass mailings without significant expense.[4] Then, the letters were sent by fax. Clearly, the Internet has once again broadened the potential to reach a larger number of 'marks' across the world, and particularly in Europe. By utilising many analogies with frauds based on letters (Buchanan and Grant 2001; Snyman 2001), the targeting strategy remained very wide; it rested more on the accessibility of lists of emails than on the specific profile of the person/enterprise targeted (Durkin and Brinkman 2009: 272). The internet version of the scam was highly practised in West Africa (Birrer et al. 2007), even if the authors were spread over the world (Durkin and Brinkman 2009).

[4] This was highlighted through specific investigations in Switzerland during the 1980s, but the order of magnitude was never studied, to our knowledge.

The virtualisation of social interactions is at the heart of the digital transformations of the frauds (Durkin and Brinkman 2009: 276–279). According to rational choice theories (Cornish and Clarke 1986), virtualisation avoids physical contact, which is a source of risk. It also makes it unnecessary to move, thus reducing the effort. Expected gains are high. Fraudsters acquire great flexibility in varying the scheme of fraud by simply changing their virtual identities. This allows them to target entirely different marks but retain the primary mechanism (e.g. advance fee fraud).

Contact can be established via various communication channels: instant messaging, phone calls, social media, specialised websites and emails. These types of environment and communication channels allow masked and asynchronous contacts. The marks can be brought into some 'hyperspace' where it becomes difficult to distinguish the virtual from the real (Durkin and Brinkman 2009).

Fraudsters use different approaches to this end, exploiting the many ways potential marks expose themselves through their routine activities (Pratt et al. 2010). By analogy with the model of the mobility triangles, initially proposed by Burgess (1925), virtual encounters can be divided into three types: *convergence*, *intrusion* and *phishing* (Fig. 1).

During a *convergence*, the author attempts to meet a mark in a third-party space used in some online activity. Typical online platforms are classified ads, sales or gaming or dating websites. They provide a context for assuming that people visiting these spaces have specific expectations, desires and beliefs, in other words, many vulnerabilities that are each a formidable lever. For example, they may involve desperately seeking companionship when in need of affection, getting a lucrative and easy job, scanning auction sites and expecting an incredible deal, being willing to spend money on the lottery, being sensitive to charity or being moved by puppies needing to be adopted (see also the next section). Among these areas of convergence, sites selling illicit products are particularly affected by fraud. Buyers are aware of the illegal

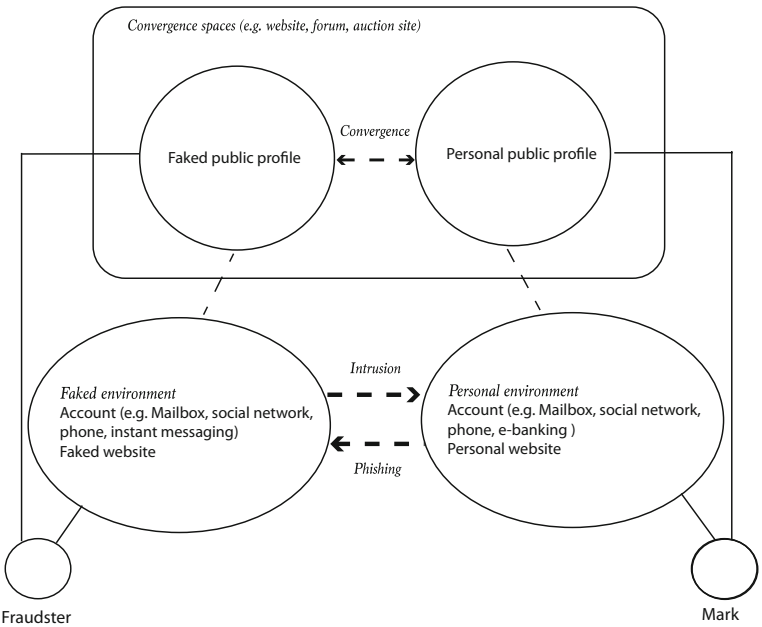

Fig. 1 Model of virtual spheres and ways of generating encounters

nature of the services (for example, the purchase of illicit drugs or counterfeit goods), which again makes them more vulnerable and unwilling to report the crime.

In cases of *intrusion*, the author enters directly into the personal space of the mark. Fraud involving fake IT support services calling a mark via telephone is of this type. For example, they use the false figure of a technician, an employee of a well-known computer company, who encourages victims to give them the keys to take control over their entire computers.

In cases of *phishing*, a fake dedicated space is presented to marks to incite them to perform certain operations or deliver personal data, facilitating different types of access (for example, a fake bank website or online store).

It is important to consider that the protagonists may move from one space to another during the fraud: for example, a fraudster may intrusively access the space of a mark by an email, which in turn incites the mark to visit a site (phishing) or another convergence space where the fraud is deployed.

Whatever the type of encounter (convergence, intrusion or phishing), the process of searching for marks ranges from highly selective (e.g. in a specific convergence space) to very broad, by placing bait. These are referred to as either targeted fraud or mass marketing fraud (Whitty 2015b).

At one extreme, some targeted fraud demands a high degree of preparation and involves the collection of personal data about marks to deploy misleading scenarios specifically adapted to their profiles. The CEO fraud, primarily conducted via telephone, is a typical example. In this fraud, the scammer steals the identity of a business owner to pressure an (targeted) employee to transfer a large sum to an account under the pretext of urgent and important business. Perpetrators occasionally also create contact with presumed marks by responding to advertisements concerning the sale of real estate. They offer much more money than requested. The perspective of substantial gain activates the seller's cupidity and greed and leads to the so-called rip-deal fraud (see above).

At the other extreme, when emails are sent in bulk (e.g. fake lotteries or many other advance fee fraud schemes), a statistical effect is expected: even if very few people believe in the scenario, a limited number of responses is sufficient to deploy the fraud. For example, when emails are sent en masse to all members of an organisation (e.g. a university) to ask for their passwords under the pretext of a problem with the messaging system, few people can be expected to answer. This is sufficient for these scammers, who are targeting access to a platform to generate a spam campaign.

Jakobsson (2016: chapters 1 and 2) rightly observes that the boundary between the targeted search of marks and mass marketing is blurred. On the one hand, a mass email could be deliberately poorly written to target the most naive. On the other hand, some fraud schemes may be implemented in a targeted or non-targeted manner (such as phishing) or involve specific groups of individuals (job seekers, etc.). Overall, the evolution of modi operandi seems to tend towards more targeting (Jakobsson 2016: 15–16), which supposedly leads to the highest profits.

Reinforce the Credibility of the Scenario and Establish Trust

When selecting marks or luring them into a trap, the scammer chooses specific contexts, depending on the fraud, to place the marks in a situation of making poor decisions by exacerbating cognitive, emotional or moral arguments that neutralise capacity for judgement. Such psychological explanations have emerged from research (Lea et al. 2009;

Kahneman 2011; Whitty 2013; Braucher and Orbach 2015). The fraudster takes advantage of these contexts to reinforce the mark's belief in the reality of the scenario and the credibility of its participants (e.g. an American soldier based in Iraq). This has been called the *grooming process*, 'given that it shares similar aspects to the way a sexual offender might groom a child' (Whitty 2013: 678). The process goes from very elaborate to useless when fraud parameters are built to immediately trigger an action from the mark. This occurs, for instance, when the fraudster has successfully usurped the identity of a figure already known by the mark (e.g. requesting help), or when an emotional or impulsive response is expected (e.g. re-dialling a premium number after having received a call from an unknown number on one's own smartphone). Within a single scam, such as a romance scam, it has been shown that the grooming process can range from very quick (several days) to rather long (e.g. 1 year) (Whitty 2015a: 449). The first confidence man, Thompson, proceeded by explicitly asking for the trust of the marks, which is another way of neutralising their defence (Braucher and Orbach 2015).

Human beings essentially make many forms of biased decisions, whereas they believe themselves to remain within social norms (Kahneman 2011; Whitty 2013). This attitude can be reinforced to the advantage of scammers in many ways in virtual environments specifically designed or operated from this perspective. Some are inspired by commercial and marketing strategies and techniques (Lea et al. 2009; Whitty 2013).

Using the mask of a person or institution of authority appears in many scenarios (Lea et al. 2009; Whitty 2013). For example, by claiming to be a member of a respectable profession, such as a doctor, IT specialist or police officer, the fraudster adopts a profile of expert or authority to weaken the position of the marks. Some other frauds are based on the illusion of a possibility, even minimal, of obtaining a substantial, life-changing gain by investing very little effort. In this type of circumstances, Kahneman (2011: chap. 29) posits that people attribute disproportionate weight to something positive (a gain) with a very low probability of occurring.

Moreover, people tend to overestimate the probability of spectacular events or, more generally, these are made easily accessible to memory. It is the art of confidence men to exploit this weakness by, for instance, profiting from extraordinary events appearing in the media (e.g. charity schemes). However, some scenarios require adaptation to specific, and occasionally temporary, victim profiles. Vulnerabilities are not evenly distributed in the population, either psychologically or from the point of view of routine activities (Whitty 2019).

The deception scheme can immediately indicate a gain that lies at the centre of the fraud (e.g. a lottery), while in other frauds, it is initially a matter of creating a climate of confidence before suddenly presenting arguments to trigger the action leading to a transfer of a value from the mark to the scammer (e.g. romance scam or rip-deal).

At this stage of the script, digitalisation again offers many new opportunities to scammers for implementing frauds that profit from a variety of psychological predispositions. Moreover, Whitty (2013: 669) reports, according to research, that communicating in virtual environments seems advantageous to reinforcing trust of the mark. The diversity of possible situations (Holtfreter et al. 2008) makes the classification of scenarios very difficult. This complexity has been modelled by Beals et al. (2015), who have classified frauds according to the expected gain underlying each scheme.

Trigger Delivery of the Asset

The fraudster evaluates when the mark is ready. At this stage, everything is prepared to trigger a transfer of goods, money or data from the mark to the fraudster. Many frauds have traditionally targeted money directly taken from the mark or transferred electronically. However, digital transformations have given an explicit value to the massive amount of data generated by human activities. The so-called Uberized business models express this change very clearly. It is therefore not surprising that many types of data are increasingly desired by fraudsters (e.g. personal data). Data can then be sold or used to obtain goods or many types of services.

While the method of obtaining the asset may vary according to the mechanism chosen by the author, cross-cutting strategies can be identified. At least three general transfer types are exploited by scammers: (1) *deliberately carried out by the mark*, (2) *without the mark knowing* or (3) *by extortion*.

Digitalisation plays an important role in each of these categories. The virtualisation of values (e.g. e-banking, value of data), digital addictions and how people make decisions when interacting in virtual environments are evidently at play when it comes to triggering the transfer of value from the mark to the fraudster.

Most frauds are based on deliberate transfers of value by marks who expect a benefit in return (e.g. good, service, money, love). In the typical advance fee scheme described above, the fraudster never stops demanding fees under many different pretexts, depending on the scenario (Durkin and Brinkman 2009). The mark must always consider the next operation as the ultimate one that will trigger the foreseen gain (near-to-win). The amounts requested are adapted to what marks are ready or able to deliver. They are often put in a situation of apparent emergency and pressure to prevent them from making rational decisions: if one does not deliver the money immediately, the gain will be definitely lost (Atkins and Huang 2013; Braucher and Orbach 2015). Overall, the technique seems analogue to the commercial strategy known as the foot-in-the-door technique. Fraudsters begin with low-cost requests, then increase the requests over time. A phenomenon of commitment is then observed that favours the continuation of payments (Freedman and Fraser 1966; Whitty 2013).

In schemes wherein money must be delivered repeatedly, such as advance fees, a turn exists that another subtle cognitive bias suffered by human beings can explain. From a positive choice that led them to engage into the game (e.g. the idea of obtaining a substantial gain), they are facing, at a certain point, a negative one. Either they leave the game and lose what has been already expended, or they continue the game but realise that the chance of achieving the expected gain is now very low. Doubt increases and fraud seems more likely for the mark each time. Arguments leading to decision-making take a turn: the engagement has reached a point where leaving the game could exert substantial negative consequences. Specific investigations reveal that marks may have already borrowed money from friends to pay scammers. Occasionally, money from the family has been used without the spouse being aware. Marks may even have stolen money from their bosses to continue the game. In such circumstances, given the high probability of losing the next sum paid and the low probability of eventually stabilising the situation, people are inclined to stubbornly cling to the little hope that remains (and not accept defeat) (Kahneman 2011). In extreme situations, some marks have preferred to commit suicide when reality had become impossible to deny or hide.

Beyond advance fees, deliberate transfer of money from marks can occur in many situations. In CEO frauds, the employee knowingly makes a payment to the account of the

fraudster under the many pretexts invented by the authors. In e-commerce, fake sellers receive payment in advance of products or services that they will never deliver. Fake buyers obtain the goods by simulating fake payment confirmations. Some swindlers also exploit overpayment strategies in the role of the buyer. The faked confirmation of payment indicates a higher amount than agreed, and the fraudster then asks the mark to return the surplus. Fake buyers may also claim that they cannot pick up the goods but will send a transport company. They pay marks with fake cheques covering both the goods and the transport fees that will be paid by duped sellers (Jones and McCoy 2014). The latter actually paid fraudsters who had usurped the identity of a carrier.

Money can also be obtained to the detriment of marks without their realising that they have transferred money. Fraud involving false technical or security problems is of this type, above referred to as a fake IT service fraud. Fraudsters call marks under the pretext of security breach, virus detection on their computer or any other technical problem. They then invite marks to install software to take control over the computer remotely. Marks are then asked to enter their bank details to acquire a software solution (e.g. an antivirus, an update of existing software). Occasionally, marks are asked to directly connect to their online banking systems. Fraudsters will eventually transfer money without marks noticing. Other scams lead victims to register involuntarily for SMS or premium rate calling services or complete online forms that require them to subscribe to unwanted services.

Finally, fraudsters can blackmail and extort money from marks. In some romance scams, victims, who have been incited to undress in front of their cameras, are threatened with the videos being posted online. In another example, in the case of false fines, the fraudster impersonates a tax department or police officer to threaten victims for prosecution for non-payment. In fake CEO scheme, fraudsters use their hierarchical position to threaten to dismiss employees if they do not transfer the money. In case of the fake sale of animals, for example, fraudsters claim veterinary expenses, transport costs or custom blockage costs. If marks refuse, fraudsters remind their prey that the animal is waiting in a small cage at customs.

Taking Distance from the Mark

Generally, fraudsters maintain a certain distance throughout the process to avoid detection, identification and localisation. They at least minimally prepare the rupture of the links with victims. Digitalisation again offers fraudsters many ways to protect themselves compared to traditional confidence games.

Virtualisation allows authors to destroy their masks (or profiles) rapidly. For instance, to create a close relationship while minimising the risk of detection, authors very quickly ask marks to move from the online convergence space (typically a social medium) to communicate directly via specific messaging systems, emails, SMS or telephone. In this way, messages and false profiles can be deleted from the platform to escape detection.

They can easily build another profile or even changes their space of operation. The link between the virtual identity and the physical person generally remains weak enough that marks cannot reconstruct it alone. Eventually, even if marks report the case, fraudsters operate without borders, and the justice system still has difficulty crossing jurisdictional lines.

Make Use of the Asset

Opportunities for laundering money following frauds have expanded exponentially with digital transformations. The virtualisation of processes and proliferation of channels for anonymous, international transactions have again expanded the number of (combination of) solutions available to the fraudsters. Their scope is impossible to describe here.

For example, case studies have shown that money laundering activity can be directly linked to a financial product. In frequent situations encountered in real cases, the process goes through money mules using their personal accounts to transfer gains. This occurs, for instance, when goods purchased by package mules with stolen data are subsequently transferred before being monetised. In this situation, money mules are actors recruited by fraudsters through advertisements which conceal the fraudulent nature of the activity. During the process, their own personal data are even occasionally stolen by the fraudsters to commit other frauds. As another example, fraudsters currently frequently target online gift cards codes that offer them many opportunities for monetisation. Indeed, unlike anonymous online payments, gift cards are easy to acquire from marks and easy to resell.

The assets obtained by the fraud fuel many types of perpetrators, from individual to criminal organisations. Anecdotally, beyond the apparent sophistication of the fraud, the money gained is sometimes immediately used for festivities and parties or for gaining social recognition. This is a well-known lifestyle among the 'grazers' who actively practice advance fee fraud from the Ivory Coast (Ladji and Bazare 2016).

Forensic Intelligence and Crime Analysis

The generic script provides a prior structure for analysing online fraud and reducing the recognition problem. It also reveals that many repetitions can be sought within the data: the same authors can use many different contexts and virtual environments to develop their frauds, and there are signs of repeated victimisation (Whitty 2019), as well as many areas of convergence concentrating certain frauds. In digital environments, using such a framework also entails not only using police reports for analysing data but also utilising more elementary and relevant information available: the traces (remnants) left by criminal activities. Traces of activities are not easy to destroy due to the complexity of Internet architectures. They thus keep a certain memory of what happened that can be exploited at all levels of a crime analysis system. Traces help to reconstruct and decipher modi operandi. They allow the linkage of entities (e.g. access to websites, use of pseudonyms, images used in scams, chronologies from dates read on messages). A forensic intelligence approach has, for instance, been exploratorily used to link activities that were previously considered separate in the area of advance fee fraud (Birrer et al. 2007). By connecting the dots, the study of traces provides a more comprehensive view of online frauds. This is indispensable when examining complex and repetitive mechanisms from a crime analysis perspective.

As a whole, such a forensic intelligence approach has already been proven successful for analysing traditional, serial crimes (Ribaux et al. 2016). The expansion of the approach to virtual spaces is not straightforward. It also provides crucial indications for treating the question of connecting virtual with physical entities. This has been concretely realised in the study of illicit markets (Rossy and Decary-Hétu 2017). In a typical example, chemical links

between illicit substances known to have been sold on the Internet with illicit products sold on the street have demonstrated the common origin of the substances (Broséus et al. 2017).

As such, the use of forensic intelligence should increase in the future, by framing the recognition or discovery of patterns using modern data mining technologies (Ribaux et al. 2016; Bollé and Casey 2018) and connecting them with the more criminological and psychological account developed here.

The Evolution of a Concrete Crime Analysis System Dedicated to Online Fraud

An integrative project has just begun to coordinate six police services in Switzerland. It illustrates the implementation of a forensic intelligence approach. The project consists of initiating a simple process of operational crime analysis, using a very simplified classification system based on the reflections presented in this paper, as well as the integration of digital traces supporting the detection of links between cases. It will be evaluated regularly but has already shown some promise, which is yet to be formalised according to the objectives mentioned here.

A preliminary evaluation study based on the cases registered by one canton's police in 2018 shows that 85% of the cases registered as online crimes are frauds. Nearly half are e-commerce frauds related to fake sellers or buyers of diverse goods. One convergence space, which is one of the main platforms for classified ads in Switzerland, concentrates 65% of all consumer product frauds. Information that has some relation to an identity for an entity (e.g. a person, an account—so-called identifying information) is used to detect links between reported cases. Eventually, basic digital traces are revealed to always be more systematically collected. Although the process is in its early stages and the dataset only covers one jurisdiction, many links have been found by analysing the data (see Table 1).

The whole dataset contains 1021 frauds reported to the police. The first percentage is the ratio of the number of identification information found on more than one case (e.g. 89 IBANs) to the total numbers of identifying information detected (e.g. 727 IBANs). Since more than one identifying information can be found in one case, the second percentage is the ratio of the number of cases linked to the total number of cases where identifying information has been found.

The stored cases are concentrated in 77 series (a series contain at least two linked cases) that have been detected. They include 464 cases (45.4% of all cases stored), which is a much higher proportion than what is typically detected for traditional, high-volume crimes (Rossy et al. 2013). The largest series contains 236 cases. Forty-four series contain cases sharing the

Table 1 Presence of identifying information in the data and number of linked cases

Identifying information	IBAN	Pseudonyms	Email addresses	Phone numbers	Websites
Number of id. information	727	694	629	593	178
N found on multiple cases	89	44	32	53	33
%	12.2%	6.3%	5.1%	8.9%	18.5%
Detected on *N* cases	524	501	411	344	136
Number of linked cases	212	100	81	141	29
%	40.5%	20.0%	19.7%	41.0%	21.3%

same modi operandi. Eighteen series contain also one or more unclassified cases (wherein the modi operandi did not correspond to one of the categories of the classification system). Thirteen series show variation of modi operandi. The two remaining series contain only unclassified cases.

Two hypotheses are formulated: (1) offenders rarely diversify their modi operandi and (2) offenders reuse the same identifiers only when they use same modi operandi. Further analyses must have been done to test these hypotheses.

Such a crime analysis system must then demonstrate that the use of the knowledge gained can help devise a (police) response.

From an Intelligence Perspective

Crime analysis involves intelligence and the practical use of information. An analysis should at least provide an indication of how to disrupt the fraud and reduce harm via preventive and repressive means. It must be considered how the alliance between criminological theories, a psychological account and a forensic intelligence approach, can be directed towards this aim. Indeed, the range of possibilities is wide on many dimensions and levels.

The understanding of each fraud as a whole allows the detection of weaknesses in the modi operandi. They open specific opportunities to use law enforcement tools. For instance, when a fraud combines physical and virtual activities (e.g. the delivery of goods purchased on the Internet with stolen data to a specific address), the police can choose to address the physical component in a way that more aligns with their traditional operations. As another example, money mules are generally weak links in the money laundering script. They are relatively easy to detect, realise late that they have been engaged in fraud, occasionally announce themselves to the police and are potentially open to collaborating during investigations. The complexity of the Internet and the augmented traceability of operations eventually provide some investigative opportunities that should not be eliminated from the range of means of action. Populations of fraudsters are not always equally careful or aware of forensic developments.

This analysis also reveals other weaknesses in the modi operandi of perpetrators. If the same fraud is attempted too often, it becomes much more visible on the Internet or in specific convergence spaces and reaches a type of saturation threshold. This translates into more efficient anti-spam tools and increased public awareness. Prevention campaigns can help enhance the effect of saturation. Police and other jurisdictions have recently made significant efforts to disseminate well-known and current modi operandi. Some photographs utilised for scams (for example, a photograph of a US soldier in Iraq or an attractive person) are easy to find on the Internet. With basic technical knowledge, police, relatives and friends can act to convince marks about the existence of fraud.

Other forms of intelligence emerge from this analysis that can potentially support the disruption of fraud. For instance, patterns of activities reflected by traces can be grasped at a technical level by monitoring systems (e.g. anti-spam) within particular computer environments (e.g. particular websites). Careful examination of the specific mechanisms deployed in each of these spaces, particularly to find marks, reveals the

possibilities of disrupting fraud (e.g. attempting to proactively distinguish faked profiles and other patterns).

These types of environments are generally specifically monitored by stakeholders outside the police who possess access to specific data. Typical examples are credit cards, auction sites or phone operators, as well as IT departments within companies. Listing the types of convergence spaces is, however, of utmost importance, because these indicate some concentration points sought in crime analysis. From a structural perspective, this activity can help police network with other stakeholders managing these environments, particularly since privacy should also be questioned when monitoring is implemented.

Cognitive biases and ways of neutralising the rational judgement of marks at various levels and steps in the process are other angles from which useful operational distinctions can be made (Kahneman 2011; Correia 2019; Whitty 2019). These potentially provide intelligence for conceiving a response (e.g. tailor-made tools for protecting and informing specific vulnerable populations or victims, or tools for persuading marks to disengage at a certain point). This is compounded by signs of repeated victimisation from certain frauds (Whitty 2019), opening opportunities for tailored and targeted prevention plans.

Eventually, other general preventive measures can be derived from the increased knowledge provided by such a crime analysis system. Relevant stakeholders, as well as the police themselves, should exploit knowledge to inform the public about how to adopt a more holistic attitude of learning to live safely in digital environments and protecting their values.

In summary, the more is known about fraud and its dynamic, the easier it is to implement this knowledge as intelligence at the strategic, operational and tactical levels. Beyond many difficulties, a wide range of legally authorised modes of action is then available for designing a response.

We must, however, admit that a significant gap remains to be filled. In addition to a lack of knowledge about the functioning of some types of fraud, hardly any knowledge exists regarding what does and does not work in terms of response.

Conclusion

The opportunities for developing innovative frauds have dramatically increased due to digitalisation. The interdisciplinary approach presented here provides insight into how these frauds have insidiously embedded themselves within digitally transformed business models, access to services and other social interactions. It presents an interpretation of the nature and extent of certain frauds' developments and, in turn, the type of vision that can be elaborated upon to design a monitoring system in a policing context.

It is indeed now expected that the police more offensively adapt to this context by developing new crime analysis processes to allow the proactive policing of online fraud. To conceive such systems, our rationality leads us to adopt a top-down approach. However, the lack of knowledge and the complexity of the problem instead favour a bottom-up attitude. In such a view, limited crime analysis components are rapidly developed and confronted with the reality of a practical environment. These

components, once validated, are then assembled into a more integrated system. By taking, as an initial step, the example of so-called confidence games, we have shown how such modest building blocks allow an improved understanding of fraud mechanisms and provided insight about how to organise the collection, organisation and interpretation of data accessible to the police. The overall objective has been to create a virtuous circle by, in turn, spurring the police to learn from certain specific online frauds. This will eventually allow them to better integrate the treatment of these frauds into their processes and improve communication with the public.

Finally, Boullier (2017) considers the trace, or remnant of an activity, to be the elementary data for analysing social phenomena in virtual spaces. By following him, a comprehensive crime analysis system should include a component that supports the detection and interpretation of traces of criminal activities on the substrate (levels/strata in computer, clouds and network architectures) upon which the fraud develops. This relates to a forensic intelligence approach that completes the criminological and psychological account which is typically dominant when it comes to discussing online fraud.

Acknowledgements We thank the anonymous reviewers who have contributed their time and expertise, which significantly contributed to the quality of the paper.

References

ABS (2016) *4528.0 – Personal fraud, 2014–15.* , Australian Bureau of Statistics, http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/4528.0Main%20Features152014-15?opendocument&tabname=Summary&prodno=4528.0&issue=2014-15&num=&view=.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(3), 23–32.

BCS (2016) *Crime in England and Wales-Year ending* March 2016, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2016

BCS (2019) *Crime in England and Wales-Year ending* March 2019, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2018

Beals, M., M. DeLiema and M. Deevy (2015) Framework for a taxonomy of fraud, Longevity Center/FINRA Financial Investor Education Foundation/Fraud Research Center, Washington DC: Stanford. , http://162.144.124.243/~longevl0/wp-content/uploads/2016/03/Full-Taxonomy-report.pdf

Bergmann, J. D. (1969). The original confidence man. *American Quarterly, 21*(3), 560–577.

Birrer, S., Ribaux, O., Cartier, J., Rossy, Q., Capt, S., & Zufferey, M. (2007). Exploratory study for the detection and analysis of links between prospective advance fee fraud e-mails in an intelligence perspective. *IALEA Journal Vol, 17*, 11–21.

Bollé, T., & Casey, E. (2018). Using computed similarity of distinctive digital traces to evaluate non-obvious links and repetitions in cyber-investigations. *Digital Investigation Vol, 24*, S2–S9.

Boullier, D. (2017) 'Big data challenge for social sciences and market research: from society and opinion to replication' in F. Cochoy, J. Hagberg, M. Petersson McIntyre and N. Sörum (eds), Digitalizing consumption, *Tracing How Devices Shape Consumer Culture*, Routeledge, London and New York.

Braucher, J., & Orbach, B. (2015). Scamming: the misunderstood confidence man. *Yale Journal of Law and the Humanities, 27*(2), 249–292.

Broséus, J., Rhumorbarbe, D., Morelato, M., Staehli, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International Vol, 277*, 88–102. https://doi.org/10.1016/j.forsciint.2017.05.021.

Buchanan, J., & Grant, A. J. (2001). Investigating and prosecuting Nigerian fraud. *United States Attorneys' Bulletin, 49*(6), 39–47.

Burgess, E. W. (1925) 'Can neighborhood work have a scientific basis? ' in R. E. Park, E. W. Burgess and R. D. McKenzie (eds), The city: suggestions for investigation of human behaviors in the urban environment, University of Chicago Press, Chicago, IL, 142–155.

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice, 32*(5), 477–493.

Button, M., C. Lewis and J. Tapley (2009) Fraud typologies and the victims of fraud: literature review, National Fraud Authority, London, http://www2.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Fraud-typologies-and-victims.pdf

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408. https://doi.org/10.1177/0004865814521224.

Caneppele, S., & Aebi, M. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing: A Journal of Policy and Practice, 13*(1), 66–79. https://doi.org/10.1093/police/pax055.

Canler, L. (1882) Mémoire de Canler, Ancien chef du service de sûreté, F. Roy, Paris.

Chinelli, A. (2019). *Analyse des escroqueries par Internet reportées à la police* Msc thesis, University of Lausanne, Lausanne.

Choi, K., Lee, J. L., & Chun, Y. T. (2017). Voice phishing fraud and its modus operandi. *Security Journal, 30*(2), 454–466.

Clarke, R. V. and J. Eck (2005) *Crime analysis for problem solver in 60 small steps*, U.S. Department of Justice, COPS, Washington, http://www.popcenter.org/learning/60steps/ (accessed August 5th 2016).

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, 44*(4), 588–608.

Cornish, D. (1994) 'The procedural analysis of offending and its relevance for situational prevention' in R. V. Clarke (eds), Crime prevention studies, Criminal Justice Press, New-York.

Cornish, D. and R. Clarke (1986) T*he reasoning criminal: Rational choice perspectives on offending.* , Springer, New-York.

Correia, S. G. (2019). Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. *Crime Science, 8*(1), 4. https://doi.org/10.1186/s40163-019-0099-7.

Cross, C. (2018) Expectations vs reality: responding to online fraud across the fraud justice network, *International Journal of Law,* Crime and Justice Vol 55, 1–12.

Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing: A Journal of Policy and Practice, 9*(2), 119–128. https://doi.org/10.1093/police/pau044.

D.H.H. (1949). The Spanish prisoner letter. *Western Folklore, 8*(3), 265.

Dupont, B. (2013) 'Skills and trust: a tour inside the hard drives of computer hackers. ' in C. Morselli (eds), *Illicit networks*, Routledge, London, United Kingdom, 195–217.

Dupont, B. (2017) 'Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime', *Crime,* Law and Social Change Vol 67 no 1, 97–116, https://doi.org/10.1007/s10611-016-9649-z.

Durkin, K. F., & Brinkman, R. (2009). 419 FRAUD: a crime without borders in a postmodern world. *International Review of Modern Sociology, 35*(2), 271–283.

EC3 (2017) *Common taxonomy for law enforcement and the national network of CSIRTs*, Europol, European Cybercrime Center.

Fischer, P., Lea, S., & Evan, K. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology, 43*(10), 2060–2072.

Freedman, J. L., & Fraser, S. C. (1966). Compliance without pressure: the foot-in-the-door technique. *Journal of Personality and Social Psychology Vol, 4*, 195–202.

Goldstein, H. (1990) Problem oriented policing, Temple University Press, Philadelphia.

Goodman, M. (2015) Future crimes. Inside the digital underground and the battle for our connected world, Anchor, New-York,

Gregg, D. G., & Scott, J. E. (2008). A typology of complaints about eBay sellers. *Communications of the ACM, 51*(4), 69–74.

Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., & Feldberg, F. (2017). Debating big data: a literature review on realizing value from big data. *The Journal of Strategic Information Systems, 26*(3), 191–209. https://doi.org/10.1016/j.jsis.2017.07.003.

Halttunen, K. (1982) Confidence men and painted women: a study of middle-class culture in America, 1830–1870, Yale University Press, New Haven.

Holt, T. J. and A. Bossler (2016) Cybercrime in progress: theory and prevention of technology-enabled offenses, Routledge, London & New York.

Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud email schemes. *International Journal of Cyber Criminology, 1*(1), 137–154.
Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189–220.
ICPC (2018) 6th International report on crime prevention and community safety: preventing cybercrime. *International* International Centre for the Prevention of Crime, http://www.crime-prevention-intl.org/fileadmin/user_upload/Publications/International_Report/ICPC_Report_2018.pdf
Jakobsson, M. (2016) Understanding social engineering based scams. , Springer, New York.
Jones, J. and D. McCoy (2014) The check is in the mail: monetization of craigslist buyer scams. Electronic Crime Research, APWG Symposium.
Kahneman, D. (2011). *Thinking fast and slow*. Londres: Allen Lane.
Ladji, B., & Bazare, R. N. (2016). Pratiques festives des brouteurs en Côte d'Ivoire. Entre ritualisation de la fête et categorisation sociale du cybercriminel. *European Scientific Journal, 12*(17, dx.doi.org). https://doi.org/10.19044/esj.2016.v12n17p198.
Laney, D. (2001) 3D data management: controlling data volume*, velocity, and variety*, Gartner Report, File 949, https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf
Lea, S., P. Fischer and K. Evans (2009) *The psychology of scams: provoking and committing errors of judgement*, Office of Fair Trading, www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf
Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology, 57*(3), 704–722. https://doi.org/10.1093/bjc/azw009.
Levi, M. (2008). Organized fraud and organizing frauds: unpacking research on networks and organization. *Criminology & Criminal Justice, 8*(4), 389–419.
Levi, M., A. Doig, R. Gundur, D. Wall and M. Williams (2017) 'Cyberfraud and the implications for effective risk-based responses: Themes from UK research', *Crime,* Law and Social Change Vol 67 no 1, 77–96, https://doi.org/10.1007/s10611-016-9648-0.
Louwage, F. E. (1932) Technique de quelques vols & Escroqueries, Anneessens, Ninove.
Loveday, B. (2018). The shape of things to come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the police service of England and Wales. *Policing: A Journal of Policy and Practice, 12*(4), 398–409. https://doi.org/10.1093/police/pax040.
Maurer, D. W. (1999) The big con, Anchor Books, New-York.
McGuire, M., & Dowling, S. (2013). Cyber crime: a review of the evidence. *Summary of key findings and implications, Home Office Research report, 75*.
Pollitt, M. (2010) A history of digital forensics. Advances in Digital Forensics VI, Berlin, Heidelberg: Springer Berlin Heidelberg,
Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267–296. https://doi.org/10.1177/0022427810365903.
Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science, 7*(1), 5.
Reiss, R. A. (1911) Manuel de police scientifique (technique). Vols et homicides, Payot Alcan, Lausanne.
Ribaux, O. (2019) 'Federalism and Swiss police reforms' in J. Janssen, K. Lünnemann, W. D'haese and A. Groenen (eds), *Cahiers Politiestudies*, Gompel&Svacina,**51,** 247–260.
Ribaux, O., Crispino, F., Delémont, O., & Roux, C. (2016). The progressive opening of forensic science toward criminological concerns. *Security Journal, 29*(4), 543–560. https://doi.org/10.1057/sj.2015.29.
Rossy, Q. and D. Decary-Hétu (2017) 'Internet traces and the analysis of online illicit markets' in Q. Rossy, D. Decary-Hétu, O. Delémont and M. Mulone (eds), The Routledge international handbook of forensic intelligence and criminology, Routeledge, Abigdon, UK**,** 249–263.
Rossy, Q., Ioset, S., Dessimoz, D., & Ribaux, O. (2013). Integrating forensic information in a crime intelligence database. *Forensic Science International Vol, 230*, 137–146. https://doi.org/10.1016/j.forsciint.2012.10.010.
Schank, R. C. and R. P. Abelson (1977) Scripts, plans. goals and understanding*: an inquiry into human knowledge*, Erlbaum, Hillsdale, NJ.
Schur, E. M. (1957). Sociological analysis of confidence swindling. *The journal of Criminal Law, Criminology, and Police Science, 48*(3), 296–304.
Smyth, S. M. and R. Carleton (2011) Measuring the extent of CyberFraud: a discussion paper on potential methods and data sources, Public Safety Canada.
Snyman, H. F. (2001). Nigerian organised crime in South Africa. *Secruity Journal Vol, 14*, 61–71.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection, 6*(1), 28–38.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime Vol, 15*, 111–129.

Vidocq, E. F. (1853) *Principal agent of the French police. Written by himself (translated from french)*, H.G. Bohn, London.

Wall, D. S. (2007) *Cybercrime: the transformation of crime in the information age. :* , Polity Press., Malden, MA.

Wall, D. S. (2010) 'Micro-frauds: virtual robberies, stings and scams in the information age' in B. S. Holt (eds), *Corporate hacking and technology-driven crime: social dynamics and implications*, IGI global, Hershey, PA (USA).

Whitty, M. T. (2013). The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665–684.

Whitty, M. T. (2015a). Anatomy of the online dating romance scam. *Security Journal, 28*(4), 443–455. https://doi.org/10.1057/sj.2012.57.

Whitty, M. T. (2015b). Mass-marketing fraud: a growing concern. *IEEE Security & Privacy, 13*(4), 84–87.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095.

Yar, M. (2005). The novelty of 'cybercrime'. An assessment in the light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.