EU CYBER VAT

Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study

---

Criminological Analysis

Deliverable 2.1

Di Nicola Andrea, Flor Roberto, Baratto Gabriele, Boriero Denise, Perrone Giulia
Centre for Security and Crime Sciences (CSSC)
University of Trento and University of Verona (Italy)

Co-funded by the European Union

EU CYBER VAT - Criminological analysis

Authors:

Andrea Di Nicola

Roberto Flor

Gabriele Baratto

Denise Boriero

Giulia Perrone

With the collaboration of (alphabetical order):

Beatrice Panattoni

Sofia Carroccia

Project: EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study

Deliverable 2.1

Beneficiary

CSSC Centro di Scienze della Sicurezza e della Criminalità — Università di Trento — Università di Verona

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Anti-Fraud Office (OLAF). Neither the European Union nor the granting authority can be held responsible for them.

Centre for Security and Crime Sciences (CSSC) of the University of Trento and the University of Verona

www.cssc.unitn.it

Trento, January 2025

Table of content

1. Introduction 3

1.1 Background 3

1.2 Objective and aim 4

1.3 Scope and methodology 6

2. The analysis 9

2.1 Clusters of *modus operandi* and actors 9

2.1 The role of ICTs: script analysis and interpretation 12

3. Conclusion 17

Bibliography 19

1. Introduction

1.1 Background

VAT fraud encompasses a variety of schemes that exploit the Value Added Tax system, broadly categorized according to their objective: reducing tax liability (tax evasion) or misappropriation of VAT through non-payment or false claims for tax credits (Fedeli et al., 2011). These frauds can be very complex, ranging from national cases to international operations with complicated "carousel transactions" that increase the financial damage to the national budget (Fedeli et al., 2011).

The fraud becomes even more damaging when several transactions are used to create multiplier effects that cause damage to the public purse through the non-payment and deduction of VAT. The issue here is twofold: firstly, the missing trader invoices VAT to its customer but does not subsequently pay it to the tax authorities, and secondly, the customer can deduct the input VAT paid to the missing trader (Lamench, 2018).

Unpaid VAT often serves as the main source of funding for criminal organizations that specialize in this category of economic and financial crime and use the funds to finance other forms of criminal activity, as will be explained later.

In the European Union a common and particularly damaging form is **missing trader intra-community fraud (MTIC)**: a complex and often **large-scale form of VAT fraud** recognized by Europol (SOCTA, 2013) as one of the **biggest organized crime threats in the EU**, affecting all Member States.

An important form of missing trader intra-community fraud (MTIC) is **carousel fraud** (CEPOL, 2022), which can be open or closed; the 'closed carousel' represents the "reference form" for this type of fraud, precisely because of this circular shape from which the name 'carousel' originates.

In this scheme, company A (supplier or 'conduit' company) in Member State 1 sells goods or services to company B (missing trader) in Member State 2. In this case, the zero VAT rate applies. Company B sells the goods and services to company C (broker) in Member State 2 and the VAT rate of Member State 2 applies. Company B then disappears without paying the VAT due. Company C then sells the goods or services back to company A in Member State 1.

The sale from company C to company A in Member State 1 is an intra-community sale and therefore company C can claim a refund of the VAT paid to company B. Therefore, the budget of Member State 2 suffers a double loss as the missing trader (company B) doesn't pay the VAT due and the intermediary (company C) claims a refund of the VAT paid to the disappeared trader.

This mechanism leads to double financial losses for the state due to unpaid taxes and unjustified VAT refunds (European Parliament, 2021).

The complexity of these schemes increases with the involvement of buffer companies, which disguise the fraudulent activities and make investigations more difficult.

Between the main actors, there may be several buffer companies, some or all of which may be honest (Smith, 2007). As for the other actors, party (C) involved may also be unaware of the fraudulent scheme, although in any case it is at an advantage by buying from the missing trader (B), as (B) can afford to sell the goods to the domestic trader at a lower price than other competing traders due to the unpaid tax it collects on recovery.

While some actors in these chains may not be aware of the fraud, the main actors — suppliers and brokers — are often complicit by using fictitious companies to commit these crimes (Tundo, 2010).

The analysis presented here focuses specifically on this type of carousel fraud as a case study because of its importance as a threat to the EU's financial interests.

Despite its significant economic and social consequences, **VAT fraud has been largely neglected in criminological research**. The field has traditionally focused on white-collar crime and corporate misconduct, **leaving a gap in the understanding of VAT fraud as a criminal phenomenon from a criminological perspective rather than an economic and legal one**. VAT fraud is becoming an increasingly complex criminal offence that poses a serious threat to the EU's financial interests, as it usually involves large companies and affects various jurisdictions inside and outside the EU market. In its 2023 Annual Report, EPPO assessed the financial impact of VAT fraud on the EU. The results show that VAT fraud accounts for 59% of the total budget lost to the EU due to the crimes investigated by EPPO and amounts to €11.5 billion, 71% more than in 2022.

Digitalisation has further exacerbated the problem and created new opportunities for fraudsters. Online transactions enable anonymity, speed and cross-border operations, making detection and enforcement more difficult (Lee & Holt, 2020). Sophisticated technologies such as cryptocurrencies and anonymous payment systems are now frequently used to disguise illicit activities, particularly in the context of e-commerce (Borselli et al., 2015).

In addition, the dematerialization of assets and transactions makes it more difficult to detect criminal activity, as it is difficult for authorities to track the flow of money and goods across the entire chain of exchange.

The **growth of e-commerce has exacerbated the risks as companies exploit the complexity of cross-border transactions** and use methods such as false reporting, failure to register for VAT and invalid VAT numbers to evade taxes (Moiseienko, 2020). The EU faces an urgent need to address these evolving threats by tackling the technological and operational sophistication of VAT fraud schemes. A deep and thorough understanding of the phenomenon is critical for law enforcement agencies to adapt and respond effectively to these challenges.

This analysis aims to contribute to this understanding by examining the **digital dimensions of VAT fraud in the European Union** to provide insights into the **criminal opportunities offered by digitalization**.

1.2 Objective and aim

The **aim** of this analysis is to **examine cyber-VAT fraud** (i.e. the digital dimension of VAT fraud) in the European Union through an empirical criminological lens. Starting from the **modus operandi as well as the characteristics of the perpetrators**, this work analyses how the **Internet affects the different activities and phases that characterize the commission of the crime of VAT fraud in the European Union**.The activity was carried out as part of WP2 "Cyber-VAT fraud: comparative criminological and criminal law analysis" of the EU-funded project "EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study". The project is conducted by the Centre for Security and Crime Sciences ("CSSC") of the University of Trento and the University of Verona with the financial support of the Directorate General for the European Anti-Fraud Office – OLAF Union Anti-Fraud Programme – EUAF. For more information on the objectives of the project, please see the box below.

As there is currently no effective and uniform definition of cyber VAT fraud, we have developed the following phenomenological definition of cyber VAT fraud to guide our analysis:

Cyber VAT fraud involves the use of technology to facilitate the criminal activity as a whole or to assist in one or more of its stages/phases. The use of technology at one or more stages/phases may include the creation of shell companies using forged documents or identities, the conduct of online transactions and the sale of online goods, including digital goods.

By 'cyber VAT fraud', the authors mean VAT fraud **facilitated by new digital technologies/elements**, as is the case in many digital organized crime activities (Di Nicola, 2022). **Digital facilitation can take place at various stages** (e.g. at the financial transaction stage, where money flows can be facilitated through online transactions); **through specific activities** (e.g. hacking to steal documents/information, creating fake documents or setting up fake companies through online channels/tools); **or through the creation of new digitally generated intangible technologies** (e.g. cloud service, software, carbon credits).

The research team, supported by institutional actors, national experts (one per Member State) and relevant stakeholders, adopted a multidisciplinary and integrated approach to assess the behaviours realised in cyberspace that could harm the EU's financial interests by evading VAT, with the aim of understanding the objective and subjective dimensions of cyber VAT fraud in the EU - the modus operandi and characteristics of the actors - with a particular focus on how digital technology is misused to commit these crimes.

The **specific aims** of the present analysis are:

a) to outline the **modus operandi** through the formation of **behavioural clusters**;

b) to outline the **characteristics of cyber VAT fraudsters** in the EU through the formation of **actors' clusters**;

c) to gain a better understanding of the **role of ICT in the commission of cyber VAT fraud** (e.g. falsification of tax documents and the creation of "fake virtual companies" used for non-existent businesses).

Project **EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study.**

General objective

The **general objective of this comparative law study** (project EU CYBER VAT) is to assess the adequacy of the current legal framework at EU and Member State level with regard to combating cyber-VAT fraud and to propose solutions to make it more effective and efficient at EU and Member State level. Using the method of comparative law research, the project will investigate whether the European criminal law framework for VAT fraud under the PIF Directive, its implementation by Member States, and national criminal law provisions can provide a sufficient level of legal protection against the intersection of VAT fraud and cybercrime. As these are cross-border and particularly serious crimes, the degree of harmonisation between national rules must always be monitored and ensured.

Specific objectives

The general objective of the project can be divided into the following 3 specific objectives (SO):

To provide an analysis of cyber-VAT frauds in the European Union from an empirical criminological point of view, with special attention to the modus operandi as well as the characteristics of the actors involved. The new threats related to the digitalization of tax transactions will be assessed from a criminological perspective, in order to provide a basis for evaluating the adequacy of measures against cyber-VAT fraud in the EU and activities to detect and investigate cyber-VAT fraud by tax and law enforcement authorities;

To provide an account of the transposition of EU criminal law into national legislations to specifically prevent and combat cyber-VAT fraud and an account of the differences between the relevant national legislations of the Member States as well as national best practices;

To elaborate, from the dual perspective of substantive criminal law and criminal procedure, recommendations and proposals to improve the EU regulation and the national anti-fraud strategies

(NAFS) against cyber-VAT fraud in order to address the new threats to the financial interests of the European Union in the context of the digital age. This will take particular account of MTIC in the digital marketplace, exploring the possibility of introducing forms of service provider accountability to prevent cyber-VAT fraud. It will also promote a higher level of harmonisation in the regulation of cross-border cyber-VAT fraud, especially when it occurs in the context of e-commerce activity.

Founding

With the financial support of the Directorate-General for European Anti-Fraud Office – OLAF Union Anti-Fraud Programme – EUAF.

1.3 Scope and methodology

To achieve the above-mentioned aims, a **qualitative methodology** was used to analyse the modus operandi of cyber VAT fraud and, in particular, a **crime script analysis** was used to distinguish the **different stages and activities** in the commission of VAT fraud and to clarify the **use of ICT in the commission of VAT fraud**. The data was extracted from **14 case studies** and **2 focus groups**, as explained in more detail below.

The **script approach** has had great success in criminological research as it sheds light on the modus operandi of offenders in committing a particular criminal activity by focusing on identifying specific criminal opportunities and explaining how they are exploited (Lavorgna, 2014). The concept of 'crime scripts' was developed by Cornish (1994) **to describe the key stages of criminal activity** and to make the decision points clearer.

For example, script analysis has mainly been used in the study of predatory crimes such as sexual crimes against women and children, robbery and theft (et al: Tremblay et al, 2001; Petrosino and Brenisilber, 2003; Smith, 2005; Chiu & Leclerc, 2017; Chopin & Beauregard, 2020; van der Bruggen et al, 2021) and in cases of check and credit card fraud (Mativat and Tremblay, 1997; Lacoste and Tremblay, 2003), employee cybercrime (Willison, 2006), migrant smuggling (Sarrica, 2005), antiquities trafficking (Weirich, 2019), wildlife trafficking (Lavorgna, 2014), terrorism offenses (Clarke and Newman, 2006), and money laundering (Morselli and Roy, 2008; Gilmour, 2014).

Various authors have used this approach to study organized crime (including: Morgenthaler & Leclerc, 2023; Chainey & Berbotto 2022; Hancock & Laycock, 2010; Chiu et al, 2011; Tompson & Chainey, 2011; Savona, 2010), as recommended in particular by Cornish and Clarke (2002).

Some authors have specifically addressed financial crime scripting by adding financial components to the crime scripting method, arguing that it provides valuable insights for analysing all forms of for-profit crime (Snaphaan & van Ruitenburg, 2024).

Few authors have examined emerging Internet-facilitated fraud using a crime script approach (Leclerc & Morgenthaler, 2023), and of the few that have specifically examined fraud facilitated by the Internet, no work was found that uses a crime script approach to analyse VAT fraud and cyber VAT fraud.

For this reason, the authors have chosen to apply this methodology to VAT fraud as it provides an effective framework for **understanding all stages of the process of committing crime** (Van Nguyen, 2022) and for understanding **how and where (at what activity/stage) the internet has facilitated this type of fraud**. Indeed, in the context of fraud, this approach provides valuable insights into the operational knowledge of perpetrators that can contribute to the **disruption of fraudulent activities**, whether they are carried out online or offline (Leclerc & Morgenthaler, 2023). In order to understand the phenomenon and to identify the criminal activities with which this type of fraud is committed, as well as to understand how *modi operandi* have changed with digitalisation, it is essential to examine **case studies**.

Indeed, this work draws on **two data collection strategies** (Hagan, 2011), namely **case studies of VAT fraud offences** (particularly court cases) where the use of the Internet played an important role, and **two online focus groups** with selected national researchers/experts and relevant stakeholders.

In terms of **sources and case selection**, relevant case studies were initially identified through a preliminary keyword search of the media, online press and online judgment database. Further cases from the different EU countries were collected through institutional contacts, in particular with authorities and officials actively involved in the fight against cyber VAT fraud (e.g. the Italian Guardia di Finanza), as well as through the national researchers involved in the project (one per Member State). A purposive sample was drawn to select the cases to be included in the analysis. Only VAT fraud that concerned Member States of the European Union and in which the Internet played a "significant" role were included. More specifically the **criteria for inclusion** in the investigation were therefore: 1) a case of VAT fraud affecting the financial interests of the EU; 2) a case of VAT fraud involving at least one cyber element; 3) the source contained details of the cyber elements of the VAT fraud and of the behaviors of the perpetrators.

On the basis of these criteria**, 12 court cases** (CC) were selected for analysis, namely 2 Italian (CC01, CC02), 3 Spanish (CC03, CC04, CC05), 3 Dutch (CC06, CC07, CC08) 1 Lithuanian (CC09), 1 Polish (CC10), 1 Czech (CC11) and 1 Belgian (CC12).

Other national experts for the remaining Member States (e.g. Greece) have pointed us to the official annual reports of the national prosecution authorities as a source of more emblematic cases.

Given the difficulty of covering all states and to find judicial cases, we also tried to extrapolate cases from the official reports of each national police authority, which we refer to as investigative cases (IC), but which we wanted to distinguish from the other court cases collected, as in many cases investigations are ongoing and we do not have the normative references.

In particular, as they met the inclusion criteria, we selected an investigative case for Greece (IC01) described in the annual reports of the Financial Police Directorate (2023) and an investigative case reported in the annual report of the EPPO (2023) that mainly concerned Spain, but the network also involved other EU and non-EU countries (IC02), so we included a total of **2 investigative cases**.

This brings the total number of cases considered to 14.

For the other countries, the national experts either did not provide us with cases (Denmark, Cyprus, Finland, France, Germany, Luxembourg and Slovakia) that met our inclusion criteria, or in many cases they provided us with newspaper articles (reporting on known cases, e.g. the Admiral case) that did not provide enough details on the modus operandi and the role of digitization (e.g. Malta) and for which no further material could be collected as they were not yet closed.

It should be noted that the publicly available case law on VAT fraud is quite limited, especially in relation to cases of fraud enabled and/or facilitated by technology. It was therefore difficult even for the national researchers involved to find suitable examples that met our research needs.

Searching for cases on the online pages of traditional newspapers and financial newspapers as well as online websites in the hope of finding articles on cases of VAT fraud also revealed descriptions of new cases, but with very limited information, particularly in relation to the digital element. Even when reviewing EPPO press releases and relevant parliamentary questions on VAT fraud, there were few findings on cyber VAT fraud.

Once the cases were identified, **cyber VAT fraud was broken down into key stages** for investigation. This was done to determine **when and how the Internet is used**. To this end, the data was analysed using a script model based on the work of Hancock and Laycock (2010) and Lavorgna (2013). Moving on to the actual script of a carousel fraud, as in Lavorgna's model “The Crime Script for Identifying Internet-

Related Criminal Opportunities" (2013), the main stages have been identified, including the stages that precede and follow the actual scam. The **ten stages** are as follows:

- Stage 1: Preparatory activities that precede the commission of the carousel fraud;
- Stage 2: Creation/opening of the "missing trader" to commit the fraud;
- Stage 3: Initial sale: intra-EU VAT-free transaction (A → B);
- Stage 4 (eventual): Multiple resales (B → Buffer(s) → C);
- Stage 5: Internal sale with VAT (B → C);
- Stage 6: Non-remitting of the collected VAT (by B);
- Stage 7: Disappearance of company B (becoming missing trader) as an exit strategy (activity to evade the authorities);
- Stage 8: Final sale: intra-EU sales without VAT returned to the first seller (C → A);
- Stage 9: Request for refund of VAT paid (by C to B, missing trader);
- Stage 10: Post-fraud activities directly resulting from or following the fraud.

The **single actions performed by the fraud actors** at each stage were identified in a general "Action" column (see Table 2), and each action was assigned a **function** using the "sequence of functions in the crime scene" identified by Cornish (1994) and described by Hancock and Laycock (2010), namely: preparation, entry, precondition, instrumental initiation, instrumental actualization, action, postcondition, and exit. Indeed, as shown in the table 2, from Hancock and Laycock 's (2010) "integrated organized crime script" model, the labels "function" and "action" were retained and a specific column "Action in which the Internet was used" was added, as in Lavorgna's model (2013).

The entire script will be explained in section 2.2 of this analysis.

2. The analysis

2.1 Clusters of *modus operandi* and actors

This section examines the **modus operandi** and the **actors involved in cyber VAT fraud**, through a detailed analysis of the selected cases.

The **ten stages** identified in the previous section represent the **course of action** we found in the VAT fraud cases we investigated, which consists of a series of behaviours aimed at planning (before), carrying out and protecting (after) a specific criminal act in order to avoid detection. The individual activities and the impact of digitalisation on them are examined in the next section.

The starting point was the identification of the main VAT fraud schemes known in the literature and the classification of those found in the case studies examined.

Traditional VAT fraud can be divided into two broad basic categories according to a classification based on the **type of scheme**, depending on whether the ill-gotten gain consists of a **reduction in the tax due** (tax evasion) or **VAT misappropriation** (non-payment of VAT due and/or false claiming of tax credits), or both (Fedeli & Forte, 2011). A further classification can be made based on the complexity of the fraud scheme: whether the fraud involves only a domestic or an international (intra-community) component, a single transaction or a chain of "carousel transactions" and how complex the carousel is (Fedeli & Forte, 2011).

As mentioned above, the most common form of VAT fraud is the so-called **MTIC (Missing Trader Intra-Community) fraud**, and an important form of MTIC fraud is **carousel fraud** (CEPOL, 2022), which is also the pattern of VAT fraud we found in our case studies (see Table 1). The following schemes can be distinguished in detail:

- **MTIC acquisition fraud** (the simplest type of MTIC fraud): company A (supplier or seller) in Member State 1 sells goods or services to company B (missing trader) in Member State 2. As this is a cross-border transaction, the zero rate applies. Company B then sells the goods or services to company C (broker) in Member State 2 and the VAT rate of Member State 2 applies. After the sale, company B disappears without paying the VAT due to the tax authorities of Member State 2 (European Parliament, 2021);
- **MTIC carousel fraud ("closed carousel")**: company A (supplier or "conduit" company) in Member State 1 sells goods or services to company B (missing trader) in Member State 2. In this case, the zero rate for VAT applies. Company B sells the goods and services to company C (broker) in Member State 2 and the VAT rate of Member State 2 applies. Company B then disappears without remitting the VAT due. Company C then sells the goods or services back to company A in Member State 1. Since company C bought the goods on the domestic market of Member State 2, it had to pay the VAT to company B (European Parliament, 2021);
- **MTIC carousel fraud ("open carousel")**: it is the same scheme as the closed carousel, with the difference that company C (broker) resells the goods to other companies operating in its country or directly to the final consumer (domestic VAT-taxable supply), deducting the VAT previously paid to company B (missing trader).

As already mentioned in the introduction, in both forms of carousel fraud, one or more buffer companies may be interposed between the missing trader (B) and company C in order to conceal the fraud from the authorities and extend the chain of fraud.

The following is an **example case description of the type of scheme** we found in each of the case studies analysed (see Table 1).

Table 1 – Type of scheme in selected case studies

Cases	Modus operandi
CC01, CC02, CC04, CC05, CC09 IC01	Misappropriation of VAT MTIC carousel fraud with a complex chain of paper companies and buffers
CC03, CC12	Reduction of the tax due Misappropriation of VAT MTIC carousel fraud with a complex chain of paper companies and buffers
CC06, CC07, CC08, CC10 IC02	Misappropriation of VAT MTIC carousel fraud with a complex chain of paper companies and buffers (also involving non-EU states)

Despite the geographical and contextual diversity of the cases, several similarities emerged in the fraudulent behaviour and characteristics of the perpetrators. These common patterns highlight the structured nature of VAT fraud and the sophisticated exploitation of systemic and technological vulnerabilities across borders. We have identified the following clusters of criminal behaviours and actor characteristics. By clustering actions and identifying roles, the analysis provides a comprehensive understanding of the strategies used by fraudsters and the interplay of actors within these schemes.

Common aspects in modus operandi - clusters of behaviours

- *Formation of shell companies*: fraudsters set up or acquire dormant companies and use false identities and documents to carry out transactions that exist only on paper;
- *Chain transactions: setting up complex networks of "missing trader" companies, which are often young and have no significant operational history or physical presence, and "buffer" companies to disguise the fraudulent activities. Buffer companies are used to extend the transaction chain, making it more difficult to detect the fraud scheme1;*
- *Fictitious transactions: no real movement of goods between buyers and sellers (non-existent transactions);*
- *Falsification or manipulation of documents: use of false declarations, forged invoices and documents to feign legitimate sales and purchases;*

[1] For example, in the Polish case - Judgment No. 466/2020 (C10) - a network of 10 interconnected entities (many of them fictitious companies) was set up to simulate a trade in hosting services. A single individual ran the network and registered and managed the domains of the entities, which had websites designed to create an appearance of legitimacy.

- *Exploitation of EU VAT rules: exploiting the rules for tax-free intra-Community supplies;*
- *Digital facilitation: the Internet is used as a tool for many activities (e.g. payments);*
- *Profit distribution: smuggling of fraudulent profits via offshore accounts or reinvestment in legitimate businesses to disguise the origin of the funds.*

Common characteristics of cyber VAT fraudsters - clusters of actors:

- *Organised groups: typically, the fraud involves individuals belonging to structured criminal organisations with different roles.*
- *Professional expertise: in other cases, the organisers are high-level individuals who hold the position of president and/or vice president of large companies and coordinate the entire fraud scheme. The "coordinators" of the fraud are individuals with expertise and professional background in tax law, financial operations, tax regulations and digital tools who join forces with each other (in the form of organised groups) to commit one or more tax crimes or with the specific aim of committing VAT fraud2.*
- *Large network of accomplices: this is a network of accomplices, including fake directors ("fronts") who act as administrators for shell companies and other intermediaries that facilitate the transfer of funds and goods.*

In relation to the authors, **three levels of participation** can be summarised as follows (Aronowitz et al., 2004):

1. **Core organisers (level 1)**: these inner circle actors plan and execute the fraud, often avoiding direct connection with the companies involved, although they receive the largest share of the profits.
2. **Outer circle actors (level 2)**: this group includes "straw men" (dummy managers), accountants, lawyers, IT specialists and other professionals who facilitate the fraud by creating fake documents or providing technical support (Middleton & Levi, 2004).
3. **Facilitators (level 3)**: Legitimate businesses, such as "buffer companies", unwittingly participate by processing VAT-exempt goods or accepting fraudulent invoices (Borselli, 2011).

At the first level, the people behind the creation or purchase of the missing trader are usually the actual organisers of the fraud. In some cases[3], in addition to the organisers, there were **operational managers** in the inner circle who ran the day-to-day operations, including preparing transactions, managing shell and filter companies, and overseeing logistics.

The organisers are usually individuals belonging to **criminal organisations** dedicated to other types of crime and using VAT fraud for capital laundering, or criminal organisations operating across borders through companies operating in several Member States (EPPO, 2023) and exploiting the VAT system for large-scale fraud. In fact, criminal organisations (especially mafia-type organisations) are becoming increasingly entrepreneurial and hide in the social fabric by penetrating the economic-productive system and intercepting the flow of funds (from individual states and the European Union) for public works or to support families and businesses. Nowadays, criminal organisations manage to obtain the necessary

[2] For example, in one of the Italian cases investigated (CC01) - Criminal judgement § 3 no. 24258/2023 - the defendants were the chairman of the board of directors, the deputy chairman and the person responsible for purchases and sales, who issued and used invoices for non-existent transactions in mutual agreement to circumvent so-called intra-Community VAT in the area of IT products (such as Microsoft Office packages).

[3] e.g. Italian Case (CC01) - Criminal judgement § 3 no. 24258/2023

financial resources by using the most advanced techniques of money laundering, tax evasion and fraud and/or by creating illicit funds through VAT fraud ("carousel fraud") (Villani, 2023). In addition, the EPPO's annual report (2022) confirms the claim that organised crime groups finance VAT fraud operations with capital derived from their other illegal activities. There are also individuals and entities engaged in money laundering that facilitate the conversion of funds from VAT fraud and other criminal activities of these groups (EPPO, 2023)

However, at the second level, we find "front men" who were often unaware of the full extent of the fraud but played a role in lending legitimacy to the fraudulent entities, and individuals with **specialised roles**, such as professional accountants, tax advisors and IT specialists[4], play a crucial role, especially as the rise of **Crime-as-a-Service (CaaS)** allows fraudsters to outsource digital expertise. For example, phishing attacks can be used to steal company data to set up bogus companies (Kothakonda et al., 2004).

Although the cases investigated had many similarities, they differed in scope and complexity. The Italian case, for example, showed a higher level of logistical sophistication and hierarchies (adopting a more 'traditional' guise of VAT fraud), while other cases showed greater sophistication in terms of the use of technology for both digital manipulation and online purchase of services (online purchase of defunct companies to convert them into paper mills[5].

In the next section, we will take a closer look at the aspects related to the use of technology and the criminal possibilities of digitalization and how these affect the different stages of VAT fraud.

2.1 The role of ICTs: script analysis and interpretation

As we have seen in the previous section, one of the recurring aspects in the cases analyzed was the "digital facilitation", where the Internet is used as a facilitator in different activities/stages of the commission of VAT fraud.

The majority of the cases analyzed primarily **involved simulated transactions** — i.e. **objectively non-existent operations**[6] — facilitated by trading in **digital goods** (e.g. hosting services[7], Microsoft Office packages[8]). The goods concerned – which are always among the goods with a high risk of VAT fraud, such as technical equipment and digital goods (cloud storage and software) – were only transferred at an accounting level, without any physical movement taking place. This was achieved through the use of simulated transactions and falsified documentation, such as fake invoices. The advent of **intangible digital goods** has made it easier to carry out such fraudulent activities. These goods can be transferred almost instantly, are more difficult to trace and do not require the same logistical infrastructure as physical goods (Masca, 2022). In the past, VAT fraud often involved low-value items (e.g. cell phones, computer chips, microprocessors, hi-fi equipment, new or used vehicles or precious metals, memory cards). However, with the increasing digitalization of VAT fraud, intangible products are becoming more common, especially in carousel fraud. These products can change hands across borders in a matter of minutes and the entire fraud process can be completed very quickly. Furthermore, as no physical logistics

[4] For example, in one Dutch case (CC07) - Rechtbank Overijssel (Nederland) No. 08/993150-19 (P) (FP) 2021 - there was a person specifically designated as "responsible for the of computerisation".

[5] Spanish case (CC04) - Supreme Court, Criminal Section, Judgment No. 675/2019.

[6] "Objectively non-existent" are called those transactions characterized by the partial or total absence of the invoiced supply or service; thus, services are invoiced that were never actually performed.

[7] Polish case (CC10) - Provincial Administrative Court in Poznaÿ, Judgment No. 466/20.

[8] Italian case (CC02) - Supreme Court, Judgment No. 24257/2023

or document monitoring (e.g. warehouse or transportation documents) is required, these frauds are much easier to carry out.

In the selected cases, "paper" companies were repeatedly set up with the aim of committing fraud or purchased on internet platforms: As mentioned above, in some cases, dormant companies with a broad corporate purpose, which were then converted into paper mills, were bought on websites offering dormant or "silent" companies for sale, even with a "straw man" person as their administrator[9].

The specialised literature also mentions the possibility of setting up "virtual companies" (Directorate of Financial Police - Annual Reports 2023, Hellenic Police) by acquiring (e.g. on the Dark Net) stolen tax data and credentials of real companies and impersonating them in order to carry out so-called **subjectively non-existent transactions**. However, we did not encounter these activities in our sample of case studies.

In addition, in some cases, undeclared accounting software was used to track real and fictitious transactions and manage "parallel markets" via separate digital registers[10].

In almost all cases, digitalization appears to have had a particular impact on the facilitation of banking transactions. Numerous bank accounts were often used and countless debit cards were managed via online banking and digital access data (codes, passwords)[11]. By exploiting home banking in particular, fraudsters were able to open and close bank accounts with great ease and speed in order to carry out fraudulent transactions while bypassing controls[12].

Finally, in all the cases analysed, we found the creation (and use) of false documents (e.g., fake invoices) and/or the manipulation of existing documents (e.g., falsifying tax returns): the goal is to create false evidence of one or more transactions in order to commit so-called objectively nonexistent transactions. It is obvious that the current digital environment has created a favorable environment for tax fraudsters to use document forgery and manipulation technologies, but unfortunately we did not find specific details on digital manipulation/falsification techniques in the various documents related to the cases analyzed.

Based on these findings, and in view of the stages described above, the data have been compiled in the following table (Table 2), highlighting for each activity of the fraudsters use of ICTs.

It must be specified that this script framework does not include all the actions required to commit VAT carousel fraud but focuses on those where the Internet was used, as found in the case studies examined. Thus, in the Table, for each stage of VAT fraud (as described in the case studies analyzed), the reader will find the various functions in the activity and the corresponding actions, as well as the type of Internet use in that specific action.

---

[9] Spanish case (CC04) - Supreme Court, Judgment No. 675/2019. In this case study, one of the defendants was being convicted of putting up for sale through the Internet inactive "dormant" companies, ready to be used in the fraud, and also a "front man" to be placed as their administrator through his website (www.sociedadesurgentes.com).

[10] Spanish case (CC03) - Supreme Court, Judgment No. 40/2020. In this case study, all these purchases (both domestic purchases and purchases to other European MS) were made by the trading department in parallel accounting records, which the company itself called 'special control', managed by the Director of the Trading Department who was responsible for 'special control'.

[11] e.g. Dutch case (CC08) - Amsterdam Court of Appeal, Case Number 23-001665-21, year 2023. In this case study, the defendant used a large number of bank accounts, with 84 debit cards and digital access data (codes, passwords) found in his possession.

[12] Dutch case (CC07) - Overijssel District Court, Case Number 08/993150-19 (P) (FP), year 2021.

In particular, the script for cyber VAT fraud outlines a **series of actions in which the Internet acted as a facilitator**. The Table (column *Action in which ICTs are used* in Table 2) shows how the possibilities of the internet are exploited, both for services (e.g. e-mail providers and instant messaging) and for online "places" (e.g. certain commercial websites) where the services needed to commit fraud can be purchased.

In the selected cases, several companies (buffers) based in different countries (sometimes even outside the EU) were always involved. However, as already explained, the use of filter companies (buffers) is not necessary for the commission of fraud, although in the analyzed cases often buffers were interposed to further complicate the tracing of the trade; for this reason, the function of this action has been referred to as 'eventual' (see Table 1).

Using this conceptual framework, it was possible to identify **five main types of criminal facilitation/opportunity that the Internet and digital society provide for the commission of this crime**, namely:

1. **Communicative facilitations/opportunities**: communication with suppliers and customers is facilitated by the use of services such as e-mail and Skype;
2. **Organizational facilitations/opportunities**: the use of the Internet facilitates the internal organization of the parties and (if any) the criminal network. The Internet eliminates the need for direct contacts with the actors involved in cross-border trade or with the end users and facilitates contacts between them;
3. **Information facilitations/opportunities**: the Internet makes it possible to access useful information and find out about certain online services that can provide solutions to specific problems. For example, the ability to obtain information about a company (e.g. VAT numbers) or to buy inactive companies to use as missing traders;
4. **Economic facilitations/opportunities**: transferring funds between bank accounts is done digitally, via online banking systems and using instant transfers, so money can be moved faster;
5. **Logistical facilitations/opportunities**: high-risk goods and digital goods are used, which can be easily moved using only accounting and simulated transactions, without the need for transportation documents or warehouses.

Table 2 - The crime script for Cyber VAT fraud in the European Union

Stage	Function	Action	Action in which ICTs are used
1	Instrumental Initiation	Identify and mapping existing service for purchasing inactive companies or identify how to quickly open a new company	Web research
1	Preparation	Formation / existence of the criminal network with other party	Online contacts (email, skype)
1	Instrumental Initiation	Recruitment of professionals (e.g. accountants, tax advisors and lawyers and IT specialists)	Online contacts (website, emails)
1	Preparation	Establishing contacts with suppliers and customers	Online contacts (online trading websites, emails, Skype)

Stage	Function	Action	Action in which ICTs are used
2	Instrumental Initiation	Creation of a fictitious company B (missing trader)	Buying inactive companies via certain websites, together with a "straw man" who is used as their administrator to exploit them for fraud
2, 3, 4 and 5	Precondition	Maintenance of contacts with other party	Online contacts (email, skype)
3	Instrumental actualization	Initial sale VAT-free (A ⟶ B)	Buying and selling in e-commerce. Buying and selling can involve digital (intangible) goods.
3	Doing	Invoicing initial sale (A ⟶ B)	Use of e-invoicing. Creation of false invoices (Internet)
3	Doing	Creation of fake documentation related to initial sale (A ⟶ B)	False purchase and sales contracts, false purchase orders and other documents with false information on transactions and business partners created using technology
4	Eventual	Multiple Resales (B ⟶ Buffer(s) ⟶ C)	Payments by express bank transfer or instant bank transfer with online banking
5	Instrumental actualization	Internal sale VAT-inclusive (B ⟶ C)	Buying and selling can take place in e-commerce. Buying and selling can involve digital (intangible) goods.
5	Doing	Invoicing internal sale (B ⟶ C)	Use of e-invoicing. Creation of false invoices (Internet)
5	Doing	Creation of fake documentation related to internal sale (B ⟶ C)	False purchase and sale agreements, false purchase orders and other documents containing false information about transactions and business partners created with the help of technology
6	Doing	B non-remitting the collected VAT	Omitting VAT declarations online

Stage	Function	Action	Action in which ICTs are used
8	Instrumental actualization	Final sale VAT-Free to initial seller (C → A)	Buying and selling can take place in e-commerce. Buying and selling can involve digital (intangible) goods.
9	Instrumental actualization	C VAT Refund Claims	Use of e-invoicing for automatic claim
7	Exit	Disappearance of Missing Trader (B)	Fast closing through access to online platforms for company registration and by completing the closing forms directly online
10	Postcondition	Dividing the proceeds of VAT fraud among all actors	Faster and anonymous economic transactions (crypto-currency, blockchains) on accounts abroad

3. Conclusion

This criminological analysis highlights the **significant and multi-layered impact of digitalisation on VAT fraud in the European Union** and provides a comprehensive understanding of **how the internet and related technologies facilitate the commission of these crimes**. By applying the script analysis method to the collected case studies, this study systematically breaks down the stages of cyber VAT fraud and sheds light on the operational techniques used by the perpetrators and the criminal opportunities offered by digitalisation.

One of the **key findings** of this study is that the **internet plays a central role in every stage of VAT fraud, from the preparatory stages to the post-fraud activities**. Digital tools and platforms streamline critical processes such as communication, the acquisition of shell companies, the falsification of documents and the execution of financial transactions.

In particular, it has been found that perpetrators often use online platforms to acquire dormant companies, usually run by straw men as administrators. These companies are sold so that they can be used as "paper companies" for fraudulent schemes. This phenomenon represents a form of industrialisation of cybercrime, where specialized individuals or organized groups create “products” (e.g. ransomware) to be sold. This practice falls under the broader concept of "Crime-as-a-Service" (CaaS), where individuals or criminal organizations that do not have the technical expertise or resources to develop specific tools (e.g. viruses or fraudulent software) can instead purchase them to carry out criminal activity more efficiently. In our case, these dormant companies were purchased and then used as "missing traders" to disguise illegal activity and evade tax liabilities.

In addition, the creation of forged documents, such as invoices and purchase orders, is further facilitated by digital tools, while instant online banking enables fast financial transfers across national borders, making it more difficult to trace and intercept fraudulent transactions.

The study also shows how digitalisation has increased the scale and complexity of VAT fraud. Unlike traditional fraud methods, **cyber VAT fraud takes advantage of the dematerialisation of assets and transactions**, reducing the need for physical goods or infrastructure. The increasing prevalence of intangible assets such as digital services and software has made it easier for perpetrators to orchestrate fraudulent activity without the physical movement of goods, relying instead on simulated transactions. This evolution in fraud methodology poses particular challenges for law enforcement agencies, as digital goods and services are more difficult to track.

In addition, the analysis confirms that **organized crime groups play an important role in VAT fraud**, often **supported by networks of professionals such as accountants, IT specialists and tax advisors**. These actors use their expertise to exploit weaknesses in the system and design sophisticated fraud schemes that circumvent detection mechanisms.

This analysis is an important step towards developing more effective strategies to combat VAT fraud as it sheds light on the phenomenon and its current manifestations. It highlights the importance of understanding the intersection between technology and crime and predicting how future advances in digitalization may further impact criminal opportunities.

Several key actions are needed to address these challenges. First, as the findings suggest that large networks of companies in multiple Member States (and sometimes even non-EU countries) are involved, there is an urgent need to strengthen international cooperation between Member States to ensure continuous information sharing and coordination of enforcement actions. Secondly, given the advanced nature of technology, investment in technological expertise is essential to equip control authorities with the necessary tools and knowledge to detect and expose sophisticated VAT fraud schemes. Thirdly, given

the speed at which goods and money can now move thanks to technology, the introduction of advanced digital tools to monitor and detect fraud in real time is essential. Together with a stronger legal framework, these tools can help close existing gaps and improve the EU's ability to respond to new threats. These aspects will be addressed in the comparative study on criminal law and criminal procedure, which will be included in the final report of the project together with this analysis.

The final report of the EU CYBER VAT project will aim to propose actionable recommendations to strengthen the EU's defenses against this pervasive and damaging form of financial crime.

Bibliography

Borselli, F., Fedeli, S., Giuriato, L. (2015). *Digital VAT Carousel Fraud: A New Boundary for Criminality.*

CEPOL. (2022). *Carousel Fraud. Serious and organised crime.* Available at: https://www.cepol.europa.eu/newsroom/news/cepol-elesson-explains-how-carousel-fraud-works-eu.

Chainey, S. P., & Alonso Berbotto, A. (2022). *A structured methodological process for populating a crime script of organized crime activity using OSINT. Trends in Organized Crime,* 25, 272–300. https://doi.org/10.1007/s12117-021-09428-9.

Chiu, Y.N., Leclerc, B. (2017). *An Examination of Sexual Offenses Against Women by Acquaintances: The Utility of a Script Framework for Prevention Purposes.* In: Leclerc, B., Savona, E. (Eds.) *Crime Prevention in the 21st Century.* Springer, Cham. https://doi.org/10.1007/978-3-319-27793-6_6.

Chiu, Y.N., Leclerc, B., and Townsley, M. (2011). *Crime script analysis of drug manufacturing in clandestine laboratories. British Journal of Criminology,* 51(2): 355-374.

Chopin, J., & Beauregard, E. (2020). *Scripting Extrafamilial Child Sexual Abuse: A Latent Class Analysis of the Entire Crime-Commission Process. Child Abuse & Neglect,* 106, 104521. https://doi.org/10.1016/j.chiabu.2020.104521.

Clarke, R.V., and Newman, G.R. (2006). *Outsmarting the Terrorists.* Westport (CT): Praeger Security International.

Cornish, D.B. (1994). *The procedural analysis of offending and its relevance for situational prevention.* In Clarke, R.V. (Ed.), *Crime Prevention Studies,* No. 3. New York: Criminal Justice Press.

Cornish, D.B., and Clarke, R.V. (2002). *Analyzing organized crime.* In Piquero, A.R., & Tibbetts, S.G. (Eds.), *Rational choice and criminal behavior: Recent research and future challenges.* New York: Routledge.

Di Nicola, A. (2022) *Towards digital organized crime and digital sociology of organized crime. Trends Organ Crim*. https://doi.org/10.1007/s12117-022-09457-y

European Parliament. (2021). *Missing Trader Intra-Community Fraud.* BRIEFING Requested by the CONT Committee, Policy Department for Budgetary Affairs, Directorate-General for Internal Policies PE 690.462 - June 2021. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690462/IPOL_BRI(2021)690462_EN.pdf.

Europol. (2013). *SOCTA EU Serious and Organized Crime Threat Assessment.*

EPPO Annual Report 2023 Luxembourg: Publications Office of the European Union, European Public Prosecutor's Office, 2024, available at https://www.eppo.europa.eu/sites/default/files/2024-03/EPPO_Annual_Report_2023.pdf

Fedeli, S., Forte, F. (2011). *EU VAT Frauds. European Journal of Law and Economics,* 31(2), pp. 143-166.

Financial Police Directorate - Annual reports 2023, Greek Police, Ministry of Citizen Protection, pp. 65-66. Available at: https://www.astynomia.gr/file/2024/03/%CE%95%CE%A4%CE%97%CE%A3%CE%99%CE%91-%CE%95%CE%9A%CE%98%CE%95%CE%A3%CE%97-%CE%94.%CE%9F.%CE%91.-2023.pdf

Gilmour, N. (2014). *Understanding Money Laundering – A Crime Script Approach. SGOC Studying Group on Organised Crime.*

Hagan, F.E. (2011). *Research method in criminal justice and criminology.* Upper Saddle River (NJ): Prentice Hall.

Hancock, G., and Laycock, G. (2010). *Organised crime and crime scripts: prospects for disruption.* In Bullock, K., Clarke, R.V., and Tilley, N. (Eds.), *Situational Prevention of Organised Crimes.* Devon (UK): Willan Publishing.

Holt, T.J., & Lee, J.R. (2023). *A crime script model of Dark web Firearms Purchasing. Am J Crim Just,* 48, 509–529. https://doi.org/10.1007/s12103-022-09675-8.

Kothakonda C., Shashikanth K., Jangalapelli S., Achi S., The challenges of cyber space with crime-as-a-service (CAAS) to amateur attackers. AIP Conf. Proc. 5 June 2024; 2971 (1) 020072.

Lacoste, J., and Tremblay, P. (2003). *Crime and innovation: A script analysis of patterns in check forgery.* In Smith, M.J., & Cornish, D.B. (Eds.), *Theory for practice in situational crime prevention studies,* Vol. 16. Monsey (NY): Criminal Justice Press.

Lamensch, M., & Ceci, E. (2018). *VAT fraud: Economic impact, challenges and policy issues.* STUDY Requested by the TAX3 Committee, PE 626.076 – October 2018.

Lavorgna, A. (2014). *Script analysis of complex criminal activities: Investigating the use of the internet as a facilitator for offline transit crimes.* In *Sage Research Methods Cases Part 1.* SAGE Publications, Ltd., https://doi.org/10.4135/978144627305013518285.

Lavorgna, A. (2014). *Wildlife trafficking in the Internet age. Crime Sci,* 3, 5. https://doi.org/10.1186/s40163-014-0005-2.

Leclerc, B., & Morgenthaler, E. (2023). *Examining emerging fraud facilitated by the internet through crime scripts. Trends & Issues in Crime and Criminal Justice,* No. 680. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77208.

Masca, S.G., Pop, A. I., *VAT Fraud in Europe - a Case Study*, 2022.

Mativat, F., and Tremblay, P. (1997). *Counterfeiting credit cards: Displacement effects, suitable offenders and crime wave patterns. The British Journal of Criminology,* 37(2): 165-183.

Moiseienko, A. (2020). *Understanding Financial Crime Risks in E-Commerce. RUSI Occasional Paper,* January 2020, pp. 2-10.

Morgenthaler, E., & Leclerc, B. (2023). *Crime script analysis of drug importation into Australia facilitated by the dark net. Global Crime,* 24(3), 169–194. https://doi.org/10.1080/17440572.2023.2212592.

Morselli, C., & Roy, J. (2008). *Brokerage qualifications in ringing operations. Criminology,* 46(1), 71-98.

Petrosino, A., & Brensilber, D. (2003). *The motives, methods and decision making of convenience store robbers: Interviews with 28 incarcerated offenders in Massachusetts.* In Smith, M.J., & Cornish, D.B. (Eds.), *Theory for practice in situational crime prevention. Crime Prevention Studies,* No. 16. Monsey (NJ): Criminal Justice Press.

Sarrica, F. (2005). *The smuggling of migrants. A flourishing activity of transnational organized crime. Crossroads,* 5(3): 7-23.

Savona, E.U. (2010). *Infiltration of the public construction industry by Italian organised crime.* In Bullock, K., Clarke, R.V., & Tilley, N. (Eds.), *Situational Crime Prevention of Organised Crimes.* Abingdon: Willan Publishing.

Smith, M.J. (2005). *Robbery of taxi drivers. Problem-specific Guides Series,* No. 34. Available at www.cops.usdoj.gov.

Smith, S. (2007). *VAT fraud and evasion. The IFS Green Budget,* 2007, p.5.

Snaphaan, T., & van Ruitenburg, T. (2025). *Financial crime scripting: An analytical method to generate, organise and systematise knowledge on the financial aspects of profit-driven crime. European Journal on Criminal Policy and Research,* 1–21. https://doi.org/10.1007/s10610-023-09571-9.

Tompson, L., & Chainey, S. (2011). *Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. European Journal of Criminal Policy and Research,* 17(3): 179-201.

Tremblay, P., Talon, B., & Hurley, D. (2001). *Body switching and related adaptations in the resale of stolen vehicles. British Journal of Criminology,* 41(4): 561-579.

Tundo, F. (2010). *Il dolo quale elemento determinante nella repressione alle frodi IVA. Corr. trib.,* No. 12/2010, p. 969.

Van der Bruggen, M., & Blokland, A. (2021). *A Crime Script Analysis of Child Sexual Exploitation Material Fora on the Darkweb. Sexual Abuse,* 33(8), 950-974. https://doi.org/10.1177/1079063220981063.

Van Nguyen, T. The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends Organ Crim* **25**, 226–247 (2022). https://doi.org/10.1007/s12117-021-09422-1.

Weirich, C., A. (2019). *Situational crime prevention of antiquities trafficking: a crime script analysis.* PhD thesis.

Willison, R. (2006). *Understanding the offender/environment dynamic for computer crimes. Information Technology & People,* 19(2): 170-186.