Project EU CYBER VAT

Criminological Analysis

Co-funded by
the European Union

CSSC
Centro di Scienze della Sicurezza e della Criminalità
UNIVERSITÀ DI TRENTO
UNIVERSITÀ di VERONA

Co-funded by the European Union

Background and needs

VAT fraud in the EU:

- Largely **overlooked** in criminology
- **Major impact**: 59% of EU budget losses in 2023 (€11.5bn, +71% vs. 2022)
- **Driven by digitalisation & e-commerce**: anonymity, speed, cross-border reach
- **Methods**: false reporting, invalid VAT numbers, non-registration
- **Urgent need** for criminological understanding & law enforcement adaptation

Aim

The **aim** of this analysis was to investigate cyber-VAT fraud in the European Union through an empirical criminological lens. Focusing on the modus operandi and the of the perpetrators, this research examined how the Internet affects the different activities and phases that characterise the commission of VAT fraud in the EU.

The **specific objectives** were:

- to outline the modus operandi (behavioural clusters)
- to identify the characteristics of cyber VAT fraudsters (actor clusters)
- to develop a better understanding of the role of ICT

Co-funded by the European Union

Scope

Operational definition: 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.

Focus: carousel fraud

Methodology

Qualitative approach, **Crime Script Analysis:**

- **data**: 14 case studies and 2 focus groups' results
- cases were broken down into **key stages** for detailed investigation to determine when and how the Internet is used during the commission of the crime
- **crime script model** adapted from the work of Hancock and Laycock (2010) and Lavorgna (2013)

Methodology

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 (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

Co-funded by the European Union

Results

Cluster of behaviours:

1. Formation of shell companies
2. Chain transactions
3. Fictitious transactions
4. Falsification or manipulation of documents
5. Exploitation of EU VAT rules
6. Digital facilitation
7. Profit distribution

Results

Cluster of actors:

1. Organised groups
2. Professional expertise
3. Large network of accomplices

Levels of participation:

1. Core organisers
2. Outer circle actors
3. Facilitators

Results

Main criminal opportunities linked to ICT:

1. Communicative opportunities
2. Organizational opportunities
3. Information opportunities
4. Economic opportunities
5. Logistical opportunities

Conclusions

Key finding: The Internet underpins all stages of VAT fraud (planning → execution → post-fraud)

Digital tools enable:

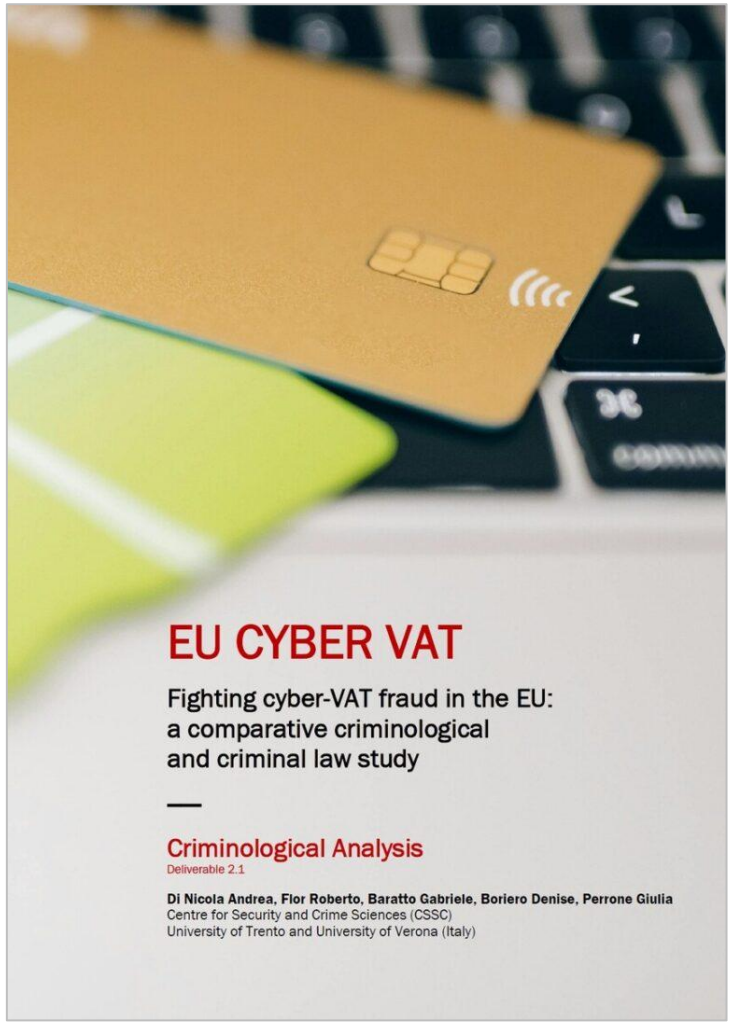
- Acquisition of shell/dormant companies via online platforms
- Forged documents (invoices, purchase orders)
- Instant cross-border financial transfers

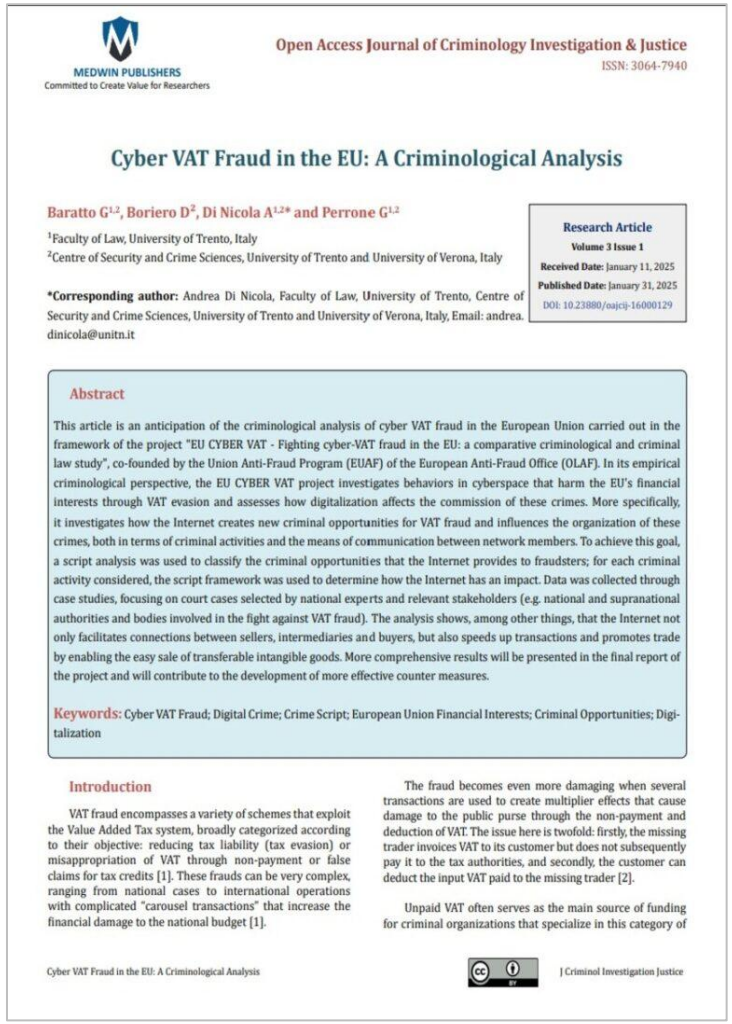
Industrialisation of crime: Dormant firms as "paper companies" → Crime-as-a-Service logic

New dimension: Intangible assets and simulated transactions increase scale & complexity

Actors: Organised crime groups + professionals (accountants, IT, tax advisers)

Detailed results





MEDWIN PUBLISHERS
Committed to Create Value for Researchers

Open Access Journal of Criminology Investigation & Justice
ISSN: 3064-7940

Cyber VAT Fraud in the EU: A Criminological Analysis

Baratto G[1,2], Boriero D[2], Di Nicola A[1,2]* and Perrone G[1,2]

[1]Faculty of Law, University of Trento, Italy
[2]Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy

***Corresponding author:** Andrea Di Nicola, Faculty of Law, University of Trento, Centre of Security and Crime Sciences, University of Trento and University of Verona, Italy, Email: andrea.dinicola@unitn.it

Research Article
Volume 3 Issue 1
Received Date: January 11, 2025
Published Date: January 31, 2025
DOI: 10.23880/oajcij-16000129

Abstract

This article is an anticipation of the criminological analysis of cyber VAT fraud in the European Union carried out in the framework of the project "EU CYBER VAT - Fighting cyber-VAT fraud in the EU: a comparative criminological and criminal law study", co-founded by the Union Anti-Fraud Program (EUAF) of the European Anti-Fraud Office (OLAF). In its empirical criminological perspective, the EU CYBER VAT project investigates behaviors in cyberspace that harm the EU's financial interests through VAT evasion and assesses how digitalization affects the commission of these crimes. More specifically, it investigates how the Internet creates new criminal opportunities for VAT fraud and influences the organization of these crimes, both in terms of criminal activities and the means of communication between network members. To achieve this goal, a script analysis was used to classify the criminal opportunities that the Internet provides to fraudsters; for each criminal activity considered, the script framework was used to determine how the Internet has an impact. Data was collected through case studies, focusing on court cases selected by national experts and relevant stakeholders (e.g. national and supranational authorities and bodies involved in the fight against VAT fraud). The analysis shows, among other things, that the Internet not only facilitates connections between sellers, intermediaries and buyers, but also speeds up transactions and promotes trade by enabling the easy sale of transferable intangible goods. More comprehensive results will be presented in the final report of the project and will contribute to the development of more effective counter measures.

Keywords: Cyber VAT Fraud; Digital Crime; Crime Script; European Union Financial Interests; Criminal Opportunities; Digitalization

Introduction

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 [1]. 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 [1].

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 [2].

Unpaid VAT often serves as the main source of funding for criminal organizations that specialize in this category of

cssc.unitn.it

Thank you for your attention!

cssc@unitn.it

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

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 Commission (Directorate General for European Anti-Fraud Office).
Neither the European Union nor the granting authority can be held responsible for them.