Assessing the Risks of Infiltration of Organised Crime in the Legitimate Economy: from the analysis to the development of a practical tool: More and Datacros projects

Ernesto U. Savona (ernesto.savona@unicatt.it)
Director and Professor (Transcrime – Joint Research Centre on Transnational Crime) Università Cattolica – Milan (Italy)

www.transcrime.it
Outline

• Project More and Datacros: one research line

• Analysing SOC infiltration in the legitimate economy in Europe (MORE)

• Looking to sectors and *modi operandi* (MORE)

• developing a tool (DATACROS) for reducing the risk of infiltration
MORE Objectives

Identifying, mapping and analysing risk factors of SOC infiltration of legitimate businesses in Europe:

- **RISK FACTORS AT MACRO LEVEL**
  - Country-level
  - Region-level
  - Sector-level

- **RISK FACTORS AT MICRO LEVEL**
  - Firm-level red flags
Definition of SOC infiltration

Any case in which a natural person belonging to a criminal organisation, as defined by Art. 1 of the EU Framework Decision on the Fight against Organised Crime (2008/841/JHA), or involved in a serious crime as defined by art. 83(1) of the Treaty on the Functioning of the European Union, or an already infiltrated legal person, invests financial and/or human resources to participate in the decision-making process of a legitimate business.

Not necessarily a crime, but a process involving a variety of sentinel crimes

Procurement regulates the allocation of resources for providing goods, services and other commodities. Infiltration of SOC enters in this area distorting through corruption the fair competition and the allocation processes.
Methodology: collection and analysis of

1. Case studies of SOC infiltration

- Criteria: OC + business
  - 50 case studies
  - 400+ firms involved

2. Data on risk factors at MACRO level

- Countries
- Regions (NUTS 2)
- Business sectors

3. Data on risk factors at MICRO level

- Accounting data
- Ownership data

- 400+ firms of case-studies
- 3000 confiscated firms in Italy
- 1300+ business ownership chains
- 20K financial reports analysed

Identification of Risk factors

- Judicial files
- Police reports
- Institutional reports
- Media sources

- 50 case studies
- 400+ firms involved

28 EU + 16 non-EU
Key findings of More project
### Sentinel crimes

#### Corruption
- Both in the public and private sector

#### Tax crimes
- As both means and objective
- Evasion of VAT, of labour contributions, of income taxes

#### False invoicing
- Also provided as services to other ‘legal’ entrepreneurs

#### Accounting manipulations
- To conceal illicit inflows/outflows and minimize income tax

#### Document forgery
- IDs, work contracts, company certifications, custom and transport bills
Case #1 (Italy)

Affiliated entrepreneurs

Cosa Nostra family

Network of businesses

Security and logistic services

False invoices

Cash

Tax evasion VAT fraud

Network of businesses
Case #1: offences

- Organised crime (not mafia-type)
- Mafia method (Art. 7)
- Private corruption
- False invoicing
- Tax evasion
- Fictitious transfer of goods/funds (intestazione fittizia)
- Money laundering

«reati economici satellite»
(Tribunale di Milano, 2017, p. 28)
Case #2 (almost identical, but in Sweden)

OCG affiliates

economic support

OCG (Bikers)

‘Homeless’
Figurehead

Provision of
Building personnel
& equipment

false invoices

cash

Colluded firms

Paying irregular
labour, tax
evasion
Modi infiltrandi

- Cash and cash-intensive businesses
- Figureheads
  - Family members
  - Figureheads ‘on demand’
- Complex corporate structures
- Secrecy jurisdictions:
  - Blacklisted countries
  - EU MS with lower transparency requirements
- ‘Golden Visas’
Business sectors / 1

- Bars & Restaurants
- Construction
- Wholesale trade
  - Food products
  - Oil products
  - Flowers
  - Medicines
- Transportation
Business sectors / 2

Healthcare
Social care

Private Security

Gaming/
VLT/Slot

Environment &
Renewable
energy

• Migrants’ assistance

• Videolottery (VLT)
• Slot machines
• Bingo
• Online gaming

• Waste management
• Wind power
• Solar power
Focus: Private security

- Evidence of SOC infiltration in various countries and by various OCGs
  - Italy, by Italian mafias and other OCGs
  - Finland, Sweden, Netherlands, Germany, by Outlaw motorcycle gangs (*Bikers*)
  - France, by Russian and Balkan OCGs
  - United Kingdom, by local OCGs
- Criminal reputation $\rightarrow$ added value for the company
- Opportunities:
  - Management of migrants’ flows
  - Loopholes in the regulation
Risk factors at MACRO level

What are the factors which facilitate SOC infiltration across territories and sectors?
Risk factors at MACRO level

**Threats**
- Corruption
- Tax crimes
- Document forgery

**Vulnerabilities**
- Cash-intensity
- Opacity of business ownership
  - Financial secrecy
  - Ownership links with secrecy countries
  - Complexity of business ownership
- Golden Visas → investment-based citizenship and residency
Risk factors at MICRO level

Financial red-flags

*Analysis of a sample of 1500 confiscated firms and peer groups of non-confiscated ones:*

- Lower financial debt
- Higher proportion of trade payables
- Higher proportion shareholders’ loans
- Higher proportion of tax payables
- Lower ratio liquid assets/total assets
- Higher proportion of *other* current assets (e.g. loans to other firms)
- Higher variance in yearly revenues
Concluding remarks

- SOC infiltration \(\rightarrow\) widespread phenomenon:
  - Variety of countries and OC groups involved
  - Involvement of brokers, entrepreneurs
  - Cross-border is key

- Common patterns and *modi infiltrandi* across countries and OCG:
  - Small firms, profitability not the priority
  - Cash still king
  - Corruption is key enabler (but investigated separately from OC?)
  - Document forgery plays key role
  - Strict links between OC and tax crimes (e.g. false invoicing)
  - OC-infiltrated firms as ‘service providers’
  - Figureheads
  - Key role of relatives (women in particular)

- Emergence of EU sectors vulnerable to SOC infiltration
Policy implications – Open debate

• Need to focus and target *sentinel crimes* of infiltration:
  – Corruption
  – Tax crimes and false invoicing
  – Document forgery

• **Reducing asymmetries** across EU MS, e.g.:
  – Cash limits and regulation across EU countries
  – Company transparency requirements
  – Investment-based citizenship and residency programs

• Increasing monitoring of:
  – emerging *vulnerable business sectors*, e.g.: gaming, private security, support to migrants
  – *intermediaries* outside the AML domain: wholesalers, import-export brokers, transportation companies

• **Developing IT tools** for improving detection of risky businesses by LEAs and AROs across countries (e.g. EBOCS)
Why Ownership structure is relevant for analyzing corruption in public procurement?

Public procurement as the privileged sector of SOC infiltration in the legitimate economy

Years ago: violence, today corruption
Identification of anomalies

› **DATACROS** is a *tool prototype* to detect anomalies in firms’ ownership structure that can flag high risk of collusion, corruption and laundering of corruption proceeds.

› It will identify the following anomalies:

1. Ownership links among companies
2. Geographic concentration of companies
3. Links with PEPs
4. Links to secrecy jurisdictions
5. Complex corporate structures
Inputs and Outputs

Accessible to authorized users only (e.g. LEASs, ACAs, etc.) -> *detailed representation of the anomalies, for investigation purposes*

Accessible to everyone -> *aggregate representation of the anomalies, for civil oversight*
Case study

› **Case:** Public procurement, road maintenance works in Sardinia

› **Year:** 2016

› **Data source:** Italian public company and contracting authority

› **Sample:** N=64 bidders

› **Focus on relational risk:**
   1. Ownership links among companies
   2. Geographic concentration of companies
Case study - Analysis

1. Ownership links among companies

2. Geographic concentration of companies

Identification of groups of connected companies

Groups obtained in 1. and 2. are overlapped

3. Overall relational risk
Results

› **Ownership links:**
  › 6 groups of companies (N=21) connected through direct or indirect ownership links
  › 3 groups of companies (N=8) connected with **strong** ownership links (TO≥10%)

› **Geographic concentration:**
  › 3 groups of companies (N=17) concentrated in small areas far from the execution of works

› **Overall relational risk:**
  › 4 groups of companies (N=22 -> 34%) with potentially collusive behavior
Data sources

1. **Ownership**: Ownership database from private providers, global coverage (e.g. *Orbis-Bureau van Dijk*). Info on: Company identifiers, ownership structure, location, sector

2. **PEP, Sanctions**:
   - Open national/local lists of PEP
   - Open national/international sanction lists
   - Lists of PEP and sanctions by private providers (e.g. *WorldCompliance* by *LexisNexis*, to be explored)
   - Other lists provided by partners

1. **Off-shore and risky jurisdictions**:
   - Official black lists (AML/CTF, Tax Havens)
   - Country risk scores (e.g. FSI by *TJN*)
   - Other lists provided by partners

2. **Procurement procedures**: Open Tender, BizPortal, other
The user selects a set of companies to be analyzed.

The various dimensions are analyzed by the software:
- Ownership
- Geographic
- PEPs
- Secrecy
- Complexity

Groups of companies with anomalous relations are identified.

Indicators of anomaly are calculated for each company in the set.

Indicators of anomaly are calculated for the whole set.
Conclusions

The two directions SOC is taking in Europe and beyond could be summarized as:

1. Traditional OC moves toward a more intensive penetration in the legitimate economy where procurement is the main area. Intensive corruption less violence

2. OC gang model is developing: more violence and corruption mainly focused at local level on Leas

Project More has analysed sectors and modi operandi of the infiltration focusing on the companies structure and concentration of the main vulnerabilities. Datacros is continuing this research-policy relevant line developing a practical tool for assessing the risk of SOC infiltration