CENTER FOR THE STUDY OF DEMOCRACY

EXTORTION RACKETEERING: THE VULNERABILITY ASSESSMENT APPROACH

Policy Brief No. 63, September 2016

Extortion racketeering has long been pointed out as the defining activity of organised crime. It has also been identified as one of the most effective tools used by organised crime in the accumulation of financial resources and the penetration of the legal economy. Although in recent years this crime has not been among the top listed organised crime threats in the strategic EU policy documents, it still remains ever present in European countries. The seriousness of the phenomenon has been recognised at the EU level and the crime has been listed in a number of EU legal acts in the field of police and judicial cooperation in criminal matters.

Extortion racketeering is a latent form of crime, infamous for the low rates of reporting by the victims. There are, however, a number of factors that hinder reporting by victims to the police – indebtedness, operating in the grey economy, fear of reprisals, lack of trust in public authorities due to their low capacity or corruption. The imminent presence of such factors results in low registration rates and authorities being unaware of the real scale of extortion rackets in their country. Standard business victimisation surveys, which are widely accepted alternative to police and judicial statistics, also often suffer from low response particularly with regards to extortion and protection racketeering and are therefore not reliable enough when it comes to assessing the full extent of the problem. For example, a recent report on the EU

KEY POINTS

- Extortion racketeering is a latent form of crime, infamous for the low rates of reporting by the victims, which result in authorities being unaware of the real scale of the problem in their country.
- The typical law enforcement approach is to investigate extortion incidents only when a victim files a report, whereas more pro-active policing and victim-focused prevention and support measures are needed in order to effectively tackle this type of crime.
- Sector vulnerability assessments could help government authorities to identify, assess and hence understand the risks related to extortion of businesses in a given economic sector.
- The vulnerability approach emphasises the examination of opportunities provided to organised crime groups by legitimate business and the broader socio-economic environment.
- The assessment of the vulnerabilities to extortion of specific sectors and social groups is a useful tool that can facilitate prevention and investigation of extortion racketeering through enhanced deterrence and detection.
- Vulnerability assessments aim at: a) ensuring better allocation of resources by competent authorities; b) informing the design of specific new policies or legislative measures; c) evaluating and adjusting administrative regulations or criminal justice tools and thus making them pertinent to the identified risks.

UNIVERSITÀ CATTOLICA del Sacro Cuore
transcrime Research Centre on Transnational Crime
UAM UNIVERSIDAD AUTONOMA DE MADRID
GUARDIA CIVIL

survey to assess the level and impact of crimes against business stated that "protection money, together with bribery and corruption, extortion and usury are part of a group of crimes that are less likely to be disclosed or declared by the respondents. For this reason, the information obtained about this type of crime could underestimate its real magnitude."[1]

The typical reactive law enforcement approach, where the police investigate extortion incidents only when a victim files a report cannot effectively tackle this type of crime. An alternative approach, currently embraced only in Italy, includes victim-focused prevention and support measures and pro-active policing, which facilitate the collaboration of the victims with the authorities and increase their resilience to extortion demands. However, in order to implement such pro-active approaches and protective measures, better understanding of this phenomenon and its hidden dynamics is required. Assessments of the vulnerabilities to extortion of specific sectors and social groups are a useful tool that can support such better informed legislative and law enforcement measures.

The vulnerability assessment approach

The vulnerability assessment approach has been developed and employed as a useful tool to identify and suggest social and situational crime reduction measures. Unlike traditional organised crime threat assessments, which usually focus on the perpetrators and the criminal markets, vulnerability assessment approach takes a holistic view of the environment and the criminal activities in order to identify vulnerability factors within the sectors – structures, relations, interdependencies, mechanisms and/or conditions that play a crucial role with respect to crime.

Vulnerability assessments usually focus on three key elements: a) environmental scanning (i.e. macro-level analysis of the environment surrounding the economic sector); b) licit and illicit sector analysis (i.e. meso-level analysis of a sector); c) analysis of organisations and counter strategies (i.e. micro-level analysis of the individual economic entity and its business processes).[2] Thus, beyond the analysis of the characteristics of the perpetrators, the suggested approach puts an emphasis on the examination of the opportunities for organised crime groups embedded in the legitimate businesses and the broader socio-economic environment.

The Financial Action Task Force (FATF) has long embraced vulnerability assessment as a tool to assess the aspects of various sectors (e.g. legal services, casinos and gaming sector, gold sector, free trade zones, etc.) that enable money laundering and terrorist financing. **FATF defines vulnerabilities** as "factors that represent weaknesses in AML/CFT[3] systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes."[4]

Elements of this approach were also integrated in the latest SOCTA report by Europol, which among other things analysed **crime relevant factors**, which are defined as "facilitating factors and vulnerabilities in the environment that have an influence on current and future opportunities or barriers for OCGs and SOC[5] areas."[6]

Key advantages

Vulnerability assessment should not be regarded as an alternative to the threat assessment approach but

[1] Dugato, M., Favarin, S., Hideg, G., & Illyes, A. (2013). *The crime against businesses in Europe: A pilot survey.* Brussels: European Commission.

[2] This is the so called MAVUS method – see Vander Beken, T., & Daele, S. Van. (2008). Legitimate businesses and crime vulnerabilities. *International Journal of Social Economics*, 35(10), 739-750.

[3] [Anti-Money Laundering/Counter-Terrorism Financing].

[4] FATF. (2013). National Money Laundering and Terrorist Financing Risk Assessment. Paris: FATF/OECD.

[5] [Organised Crime Groups and Serious and Organised Crime].

[6] Europol. (2013). *SOCTA 2013: EU Serious and Organised Crime Threat Assessment.* The Hague: Europol.

as an important complementary component of crime risk analysis. Furthermore, with regards to organised crime activities with high latency and low reporting rates by the victims such as extortion, it could provide a viable venue for detection and tackling through better understanding of the environment where it occurs and the existing opportunities it exploits in the different sectors or communities.

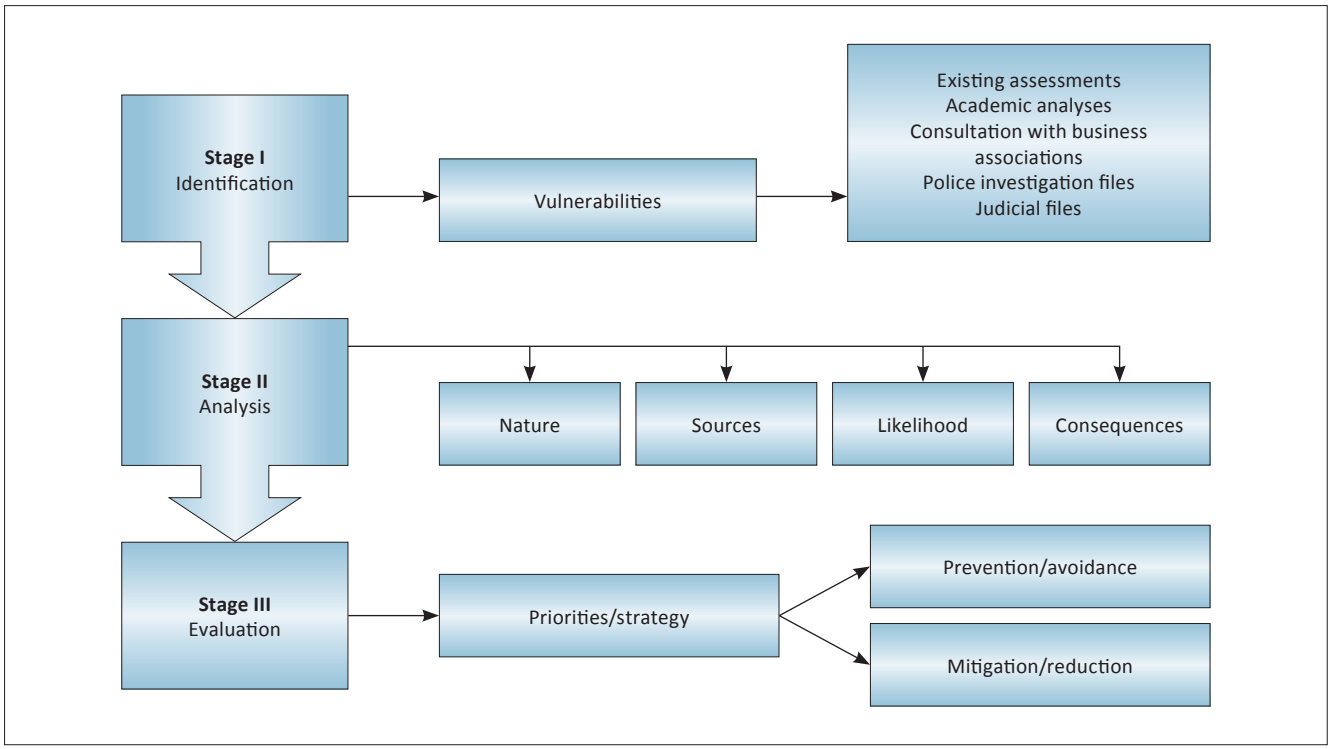
The **key advantages** of the sector/community vulnerability assessment is that it allows for a tailored approach, which helps to identify sector-specific or community-specific factors enabling or facilitating extortion. Thus, it can also suggest tailored red flag indicators to facilitate early detection and specific prevention and mitigation countermeaures against those aspects of a specific socio-economic context or migrant communities which provide opportunities for crime.

The **ultimate purpose** of such assessment is to facilitate prevention and investigation of extortion racketeering through enhanced deterrence and detection. The **specific objectives** of such an assessment include: a) to ensure better allocation of resources by competent authorities; b) to inform elaboration of specific new policies or legislative measures; c) to evaluate and adjust existing administrative regulations or criminal justice tools and thus make them pertinent to the identified risks. Certainly, in order to contribute to a sustainable impact on the proliferation of extortion such an assessment should be embedded in the overall risk management process of strategic planning, policy implementation, measurement of results and subsequent re-evaluation.

Method for assessing vulnerability to extortion of specific sectors

The study *Extortion racketeering in the EU – vulnerability factors*[7] elaborated and piloted a method for

Figure 1. Overview of the vulnerability assessment process



Source: *Adapted from FATF, op.cit.*

[7] Center for the Study of Democracy. (2016). *Extortion racketeering in the EU: vulnerability factors*. Sofia: CSD.

assessing sector/community vulnerability to extortion, which generally adapted the model for crime risk assessments suggested by FATF.[8] The elaborated method follows three stages of assessment: identification, analysis and evaluation.

The **identification stage** is descriptive and draws up a list of potential vulnerability factors that enable or facilitate extortion racketeering of businesses in a specific economic sector or community. The second stage (**analysis**) brings a holistic understanding of the nature, extent and possible impact of the identified vulnerability factors. The last stage is the **evaluation**, where the risks analysed are assessed as a whole in order to determine the priorities for addressing the risk and subsequent measures for prevention and/or mitigation of risks.

Stage 1: Identification of potential risks and vulnerabilities

Once the purpose and the scope of the vulnerability assessment have been established, the first step is to **identify the vulnerability factors**. The factors that should be considered at this stage include such related to the environment surrounding the sector/community, the sector/community itself and the individual economic entities and their business processes. In order to take into account all these aspects, a combination of data collection approaches is needed.

Table 1. Sample vulnerability indicators

Factors related to the environment	Factors related to the economic sector
• 'Hot spots'/main regions affected; • Protective measures adopted by the government, business associations; • Level of the shadow economy; • Level of corruption; • Rates of employment/unemployment; • Size of the population; • Main economic sectors; • History and presence of organised crime.	• Regulatory gaps; • Number of companies operating in the sector; • Structural characteristics (i.e. share of big companies vs SMEs); • Business associations active in the sector.
Factors related to specific migrant communities	**Factors related to company owners/executives and their business**
• Size of the community; • Number of companies operating in the community; • Presence of active business/community associations; • History and presence of ethnic organised crime in the community; • Level of trust in national law enforcement authorities; • Cultural traditions discouraging external interference in the community.	• Age of victims; • Gender of victims; • Nationality of victims; • Role in the company; • Location and type of legal entity; • Number of employees; • Core activity of victimised company; • Business association membership; • Use of private security services; • Duration of extortion; • Reporting to police forces; • Reaction to extortion; • Relation with extortionists; • Economic status of the business after the extortion.

[8] FATF, op. cit.

The method for assessing sector/community vulnerability to extortion suggests as a starting point of the identification phase the collection of information on existing and known extortion incidents involving companies in the sector which is subject to assessment. The information from such incidents can be then scrutinised in order to identify recurring characteristics of perpetrators, business entities affected (e.g. size of company, number of employees), as well as recurring spatial (e.g. 'hot spot' zones), temporal (e.g. behaviour of victim at the different stages of the extortion), or other relevant specifics.

Data on such incidents could be retrieved from police and judicial files, containing official results from investigations carried out (i.e. from wiretaps, testimonies by collaborators with justice, witnesses and victims, patrimonial investigation and analysis of documents seized from criminal groups). Information on the incidents could be further augmented through approaching police officers and prosecutors that have dealt with these cases and reviewing the publicly available information from media sources. Victimised business managers and owners, as well as business associations could also be a useful source of information. This bottom-up approach is specifically useful in the identification of vulnerabilities related to the economic sector and the individual economic entities and their business processes.

Since only some of the vulnerabilities pertain to the victimised economic entities themselves, the second step in the identification of the vulnerability factors should be to examine the factors related to the sector under assessment and the broader political, regulatory, economic and social context at national level. Once the previous or ongoing extortion incidents have been identified and most affected regions ('hot spots') have been determined, complementary information could be sought in order to examine the specific regional/local context as well. Possible sources of such data are existing analyses, publicly available statistics, consultations with relevant regulatory authorities and business associations.

Overall, four sets of factors should be explored in order to draw a comprehensive set of vulnerability indicators: a) the broader political, economic, social and legal environment; b) the sectoral or community specifics; c) the specific characteristics of the victimised companies; d) the specific characteristics and *modi operandi* of the perpetrators (see Table 1).

Stage 2: Analysis

The second step suggested within this method for assessment of sector vulnerabilities to extortion **is the analysis stage**. The analysis examines the differences and similarities between the identified extortion incidents, enabling and resistance factors, existing measures and strategies to support victims and fight extortion. It then produces an **indicative list of red flag indicators** that could help early identification and specific countermeasures to target extortion racketeering.

The analysis of the data collected within the study *Extortion racketeering in the EU: vulnerability factors* has produced **three sets of red flag indicators about vulnerabilities**: a) red flags in the agricultural sector; b) red flags in the tourist sector; and c) red flags about Chinese communities (see Table 2). The red flag indicators can generally be categorised in 4 types of vulnerabilities: 1) such deriving from the general socio-economic, regulatory and legal environment; 2) such deriving from the economic sector specifics; 3) such related to the business processes of the victimised companies; 4) such deriving from community specifics (see Table 2).

In order to assess the risk of extortion racketeering stemming from the identified vulnerabilities, the assessment should also take into account the consequences of extortion racketeering. For example, the following consequences have been identified for the agricultural and hospitality sectors:

1) Agricultural sector:

- Increased exiting by small and medium farm holdings from the sector;
- Increased unemployment in rural regions;
- Depopulation of rural regions;
- Loss of agricultural traditions;

Table 2. Vulnerability factors in hospitality, agriculture and Chinese communities

Vulnerability factors	Nature of vulnerability	Hospitality	Agriculture	Chinese communities
Areas with high density of small businesses	Environmental	√	√	√
Culture of illegality/traditional presence of organised crime	Environmental	√	-	-
Deep-rooted corruption in regulatory bodies	Environmental	√	√	-
Weak and inefficient regulatory bodies	Environmental	√	√	-
Cumbersome and complex legislation/ poorly designed regulations	Environmental	√	-	-
Regions where the sector provides the only viable source of incomes	Environmental	-	√	-
Spread of grey economy practices (tax evasion, use of undeclared labour)	Environmental/ Sector specific	√	√	√
A significant share of small and medium enterprises	Sector specific	√	√	√
Low market entry barriers due to low level of capital, technology and expertise required	Sector specific	√	√	√
Cash being the predominant form of payments	Sector specific	√	√	√
Profits and outputs are easy to monitor by potential extortionists (e.g. number of clients, size of farmed land)	Sector specific	√	√	√
The businesses are territorially bound (they cannot be moved somewhere else easily)	Sector specific	√	√	√
Regulations of CAP funding	Sector specific	-	√	-
Land restitution and privatisation	Sector specific	√	√	-
Food market concentration	Sector specific	-	√	-
Mistrust of national law enforcement and regulatory authorities	Community specific	√	-	√
Hermetic nature of migrant communities	Community specific	-	-	√
Dependence of the small and medium farm holdings on external financing	Related to business processes	-	√	-
Lack of awareness in institutions/ victims about the new forms of extortion	Related to business processes	√	√	-

- Decrease in national food security and growing dependency on import of foods;
- Negative environmental impacts.

2) Hospitality sector:

- Reduction of investments;
- Increased presence of OCGs/money laundering;
- Decrease of economic competitiveness;
- Increased corruption levels.

The identified vulnerability factors could be analysed applying a common risk analysis matrix accounting for the likelihood that a vulnerability would be exploited by extortionists and the potential consequences that this creates. Thus, they can be assigned values on the basis of the risk they pose – i.e. low, medium, high.[9]

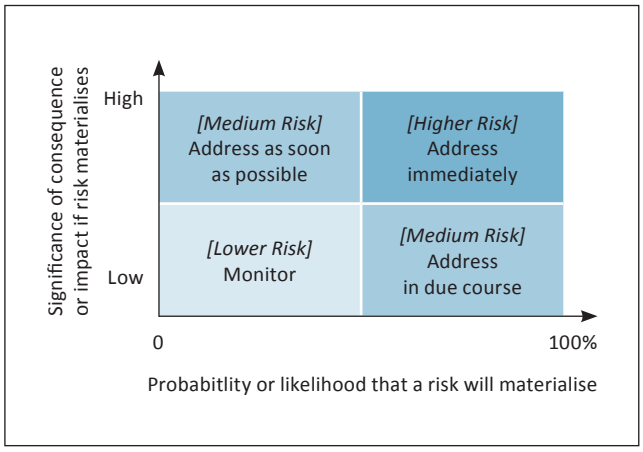
[9] Here, the red flags and recommendations have not been ranked, since any ranking would need to take into account the specific national context and be tailored accordingly.

Stage 3: Evaluation

The last step suggested within the method for assessing sector/community vulnerability to extortion is **evaluation**, which is supposed to determine the priorities and specific measures for addressing the risks, which have been identified and ranked within the second stage of the vulnerability assessment. Based on that a strategy and/or action plan to prevent/mitigate the identified risks could be developed.

Depending on the source, nature, likelihood and consequences of the identified vulnerabilities a number of measures for addressing the risks can be considered and planned – including preventive measures, mitigation measures and contingency measures. Subsequently, these could be determined for immediate, short term and long term implementation (see Figure 2).

Figure 2. Vulnerability evaluation matrix



Source: *Adapted from FATF, op.cit. p. 2.*

The report *Extortion racketeering in the EU: vulnerability factors* suggests the following list of measures, drawing on the vulnerabilities identified:

- awareness raising about the new forms of extortion within law enforcement and criminal justice authorities through trainings and exchange of experience;
- reaching out to vulnerable businesses through information campaigns and establishing help desks or hot-lines;
- encouraging and supporting business and civil society organisations that could provide assistance to victims of extortion and foster collective resistance at the local level, including provision of financial support to such organisations;
- providing support and protection to victims of extortion through establishing mechanisms for financial compensation and enhancing victim protection measures;
- closing up existing loopholes and harmonising existing regulations concerning the specific sectors (e.g. farm subsidy regulations for agriculture and food safety regulations for hospitality, etc.);
- enhancing anticorruption measures within police and regulatory bodies overseeing the specific sectors.

In addition to the general policy recommendations, the report pointed out several specific ones with regards to fighting extortion racketeering in the Chinese communities. These measures involve:

- implementation of community policing strategies within such ethnic groups;
- provision of specialised training to police officers for enhancing their cultural sensitivity and better understanding of the nature of intra-ethnic extortions;
- recruiting and training of police officers of different nationalities;
- exchanging experiences in investigating intra-ethnic extortions.

BULGARIAN-SWISS COOPERATION PROGRAMME
БЪЛГАРО-ШВЕЙЦАРСКА ПРОГРАМА ЗА СЪТРУДНИЧЕСТВО

This publication was made possile by the support of the Swiss-Bulgarian Cooperation Programme

Co-funded by the Prevention of and Fight against Crime Programme of the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of its authors, and the European Commission cannot be held responsible for any use which may be made of the information contained therein.