LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

M.A. in International Relations, Department of Political Science

Chair of Security Studies

Master's Dissertation

Organised crime in Europe. A case study of the "Russian Organisation" ("Rossijskaja Organizacija")

Supervisor: Gen. Carlo Magrassi

Co-supervisor: Prof. Igor Pellicciari

Candidate: Ludovico Ninotti (634162)

ACADEMIC YEAR 2018/2019

ACKNOWLEDGEMENTS

I would like to thank my supervisor General Carlo Magrassi, as well as my co-supervisor, Professor Igor Pellicciari, for agreeing to support the choice of the topic I decided to enquire in this thesis. Moreover, I would like to thank Colonel Cesario Totaro and Doctor Simone Pasquazzi for the valuable advices and information provided, as well as for putting me in contact with key experts of the sectors analysed in the research. In addition, I am indebted to Professor Irina Dovizova for her useful suggestions in the consultation of the Russian linguistic resources. Furthermore, I am grateful for the opportunity I had to conduct a research period at Telsy SpA in Rome, which allowed me to observe and have a first-hand experience of some of the aspects analysed in the thesis.

TABLE OF CONTENTS

INTRODUCTION

In the present research is conducted an overview of organised crime in Europe and the activities and sectors in which it is involved, completed by a detailed analysis of the infiltration of the Russian organised crime (*Rossijskaja Organizacija*) in Europe. The choice of this case study has been driven by two main factors: the serious threat posed by the phenomenon in analysis to the European security and the ability of Russian criminal groups to contaminate the political and economic spheres in Europe. As far as the method employed in the present thesis is concerned, it is worth mentioning that the research was based not only on the scientific literature on the subject, reports and analyses made by European Union's agencies and public and private organisations, but on the consultation and interpretation of official documents released by the Russian Federation. Moreover, in specific aspects analysed, such as the cybersecurity dimension of the threat placed by Russian cybercrime, the present thesis benefitted of the three-month research period conducted by the author in *Telsy*, a cybersecurity company classified among the strategic enterprises for the security of the Italian Republic.

Organised criminal groups in Europe have evolved through the years, renouncing to high visibility and ruthless violence, acquiring instead a new profile based on the deep infiltration into the societal tissue. The current trend of organised crime is that one of a complete *mimesis* with the ordinary structure of a society. A profound infiltration into the economic and political domains of a country is the main aim of a sophisticated organised criminal group, whose strength lies in the ability to shape the political and economic choices of a country, be part of the "establishment", influence and give direction to the future developments of the society for personal benefits. Organised crime is a plague infecting our societies, which is becoming more difficult to detect clearly, due to the fact that, especially in the last years, it has turned its attention to the legitimate economy. A current and threatening paradigm to which organised crime can be ascribed is that one of a cohabitation with the political and economic structures of a society, a pattern whose realisation has been possible through deception and corruption mechanisms. On the other side, organised crime persists to operate in the traditional illegal markets, which cause harm and economic loss to the society. Nevertheless, the most serious threat to the European security architecture is placed by the operations carried out in the legitimate economy, rather than the activities within the illegal markets, for a number of reasons, among which the fact that when infiltrating the legal economy, organised crime is more difficult to detect and the line between what is legal and what is not become blurred. This is exactly the aim of a successful organised criminal group, the creation of "grey zones", where it becomes difficult to distinguish illicit operations from licit ones, due to the establishment of a complex and sophisticated architecture based on connections, corruption and political ties.

The argument presented in the present research is that organised crime is a distorted form of governance, which affects and undermines the sound development of the society. Then, as far as the case study of the infiltration of the *Rossijskaja Organizacija* is concerned, the main hypothesis sustained in the thesis is the presence of a strong connection between the *Rossijskaja Organizacija* and the Russian state, that exploits the

Russian criminal networks in Europe as a tool to pursue its geopolitical agenda and as a mean of the *Informacionnaja Vojna* ('Information Warfare') against the West, in the context of the struggle for the imposition of an hegemonic cultural paradigm, between the European and Eurasian models.

Considering Europe, the present research adopted the interpretation of Varese, according to which organised crime is a form of governance as the mafia and the State, since its main characteristic is the ambition to govern exchanges, the supply of protection and impose control over them[1]. In the first chapter, the main characteristics of organised crime in Europe are presented as well as the main activities carried out and the profits thereof. One of the most lucrative illegal markets is that one of the illicit drug trafficking that generates €24 billion euros per year[2], which is just one facet of the phenomenon. Other activities carried out by organised crime groups in Europe involve migrant smuggling, trafficking in human beings, illegal trafficking of firearms, cyber-related crimes, economic crimes, property and environmental crimes. All these activities, with their specific *modus operandi* and characteristics, constitute a considerable risk for the State as well as for the economic governance of a country. Moreover, what results to be most threatening for the European security is the challenge placed by the infiltration of organised crime in the legal economy and the effects thereof. Taking into consideration the *Rossijskaja Organizacija*, a fundamental dimension that needs to be discussed to understand its contemporary outlook is related to the historical and cultural background of the phenomenon. For this reason, an historical *excursus* is provided in chapter two, since the origin of the contemporary *Rossijskaja Organizacija* traces back to the tradition of the *vory v zakone* ('thieves-in-law'), which emerged during the Soviet times from the development of a criminal subculture that was already present during the Tsarist years. The analysis of the historical origins is relevant for a number of factors, among which the capacity of the *Rossijskaja Organizacija* to adapt itself to the changing conditions of the society, its metamorphic nature as well as for the persistence of old traditions such as the use of a common fund ('*obščak*') – to which all the members of the criminal community had to pay a contribution, that is still one of the characteristics of Russian organised criminal networks – and to highlight the relevance of the prison system, where the *vory v zakone* originated, that is still nowadays a preferential site for recruitment of new members and for the forging of alliances. In this context, another aspect has been investigated in the present research, that one of the language. As observed by Whilelm von Humboldt, a language is the phenomenal manifestation of the spirit of the people[3], therefore, according to the Prussian scholar, to understand a nation it is fundamental to know the language, since it represents the way a people perceive the reality and elaborate about themselves and the others. This interpretation can be applied to specific social groups as well and, in this thesis, it has been applied to the Russian criminal language, the so-called *ofenskij jazyk* or *fenja*, whose origin traces back

[1] Varese Federico, "What is organised crime?", in F. Varese (ed.), *Organized Crime: Critical Concepts in Criminology*, (London: Routledge, 2010).

[2] United Nations, International Narcotics Control Board, "Chapter III: Analysis of the World Situation" in *Report 2017*, January 2018.
Available at: https://www.incb.org/documents/Publications/AnnualReports/AR2017/Annual_Report/E_2017_AR_ebook.pdf.

[3] Von Humboldt Wilhelm, "Latium und Hellas oder Betrachtungen über das classische Alterthum", in *Ausgewählte Schriften* (Berlin: Zenodot Verlagsgesellschaft mbH, 2014).

to the Middle Ages and that, even if radically transformed throughout the centuries, is still spoken within the Russian criminal community. A detailed study of the *fenja* is provided and the main reason behind this choice lies in the fact that paying attention to *fenja* and the criminal jargon means to acquire a more comprehensive and profound knowledge of the Russian criminal phenomenon, since the language is both a sociological and psychological phenomenon, that provides to the observer valuable information about the speaker, his or her sociocultural extraction, geographic origin, believes, attitudes and mentality, thus constituting also a valuable mean to understand criminal strategies and targets. Therefore, an analysis of the contemporary words employed in the *fenja* language – completed by the etymological root and translation in both Russian and English – in the different sectors of the illegal activities is provided, as well as a discussion over the specific terminology employed to identify the specialisations within the criminal networks and of the words and expressions used to indicate the different branches of the law enforcement authorities. Furthermore, the cultural analysis is also extended to other distinct features of the *Rossijskaja Organizacija*, namely the symbology of the criminal tattoos, which characterised Russian criminals in the origin and that are relevant to understand the Russian criminal subculture, whose traits are still partially preserved in the contemporary outlook of the *Rossijskaja Organizacija*.

Then, in chapter three, is analysed the infiltration of the *Rossijskaja Organizacija* in the European economic sectors, under a specific hypothesis proposed in the thesis, that one of the "criminal-governmental nexus" between Russian organised criminal groups on the one hand, and Russia's state apparatus on the other. This specific connection in the Russian context has profound influence over the presence of the *Rossijskaja Organizacija* in Europe and it represents a fundamental aspect, that needs attention in order to understand and counter the threat posed by the phenomenon within Europe. In fact, the origin of Russian organised crime lies in the power *vacuum* left by the collapse of the Soviet Union in 1991 and in the illness of the dysfunctional State emerging in the transition from a state-run to a market economy in the following years. In the aftermath of the fall of the Soviet empire, organised criminal groups emerged as a response to the deficiencies of the state, acting as providers of protection and services, which the State was unable to offer to its own citizens, in a context of widespread corruption and uncertainty. The critical condition of the post-Soviet years in Russia led to the affirmation of a hegemonic power exercised by organised criminal groups over the Russian society, which abandoned street violence and intimidation and turned to the business sector, taking advantage of the opportunities opened by the transition to a market economy and shaping a new societal class of business-entrepreneurs holding the economic power in Russia, widely known as oligarchs, whose posture remained uncontested until the rise to the power of Vladimir Putin in the 2000s. As a matter of fact, Putin reorganised the relationship between the State on the one side, and organised crime on the other, through a process of "nationalisation" of the criminal underworld, completed by the introduction of the *vertikalnaja sistema* ('vertical system'), which refers to the partial nationalisation of the strategic industrial sectors (e.g. energy) and the establishment of a new relation between the State and the criminalised business sector, that was compelled to agree on a new type of cooperation based on the subordination to the state apparatus. As a result,

part of the oligarchs agreed to this new pact with the State and were gradually absorbed into public institutions, while others preferred to move their assets abroad, due to the volatility of the Russian economy and the new and powerful grip exercised by the Kremlin. For these reasons, a considerable amount of Russian capital of unclear origins was increasingly invested into the European market, where the *Rossijskaja Organizacija* specialised in money laundering operations, elaborating sophisticated mechanisms such as the so-called "Russian Laundromat", a money laundering scheme of transnational nature, which allowed criminals and corrupted politicians to move over US$ 20 billion dollars from Russian banks to Moldincobank in Moldova, where the money were first "washed" and then sent to Latvia and other European countries. Another example of the penetration of the *Rossijskaja Organizacija* in the European legal economy and the presence of the "criminal-governmental nexus" is represented by the "Magnitskij affair", a money laundering case of 2006 perpetrated against the Hermitage Capital Management (HCM), a foreign fund operating in the investment sector in Russia, owned by Bill Browder, a British businessman. A case, analysed in the present research, that clearly shows the money laundering activities carried out by Russian criminals as well as the protection provided by the state to those operations. Other relevant cases which demonstrate the level of penetration of the *Rossijskaja Organizacija* in the European legal economy are taken into consideration with a specific focus on the activities carried out in Germany, Italy and the Baltic countries. Specifically, the German case is analysed to point out the organisational structure of the *Rossijskaja Organizacija* in Europe – characterised by a flexible and not strictly hierarchical nature made of loose multi-ethnic networks – and the extent of the threat represented by Russian cybercrime, responsible of over 52.9% of the cybercrimes committed in Germany in 2017, according to the Bundeskriminalamt (BKA)[4]. Then, the infiltration of the *Rossijskaja Organizacija* in Italy is analysed specifically to highlight the preferential sectors of investment in the European legal economy (e.g. real estate) and to underline the *modus operandi* of Russian criminal groups, which do not try to impose control over a given territory but just to generate profits, due also to the strong presence of autochthone criminal groups in Italy. Furthermore, in the case study of the infiltration of the *Rossijskaja Organizacija* in Italy, a divide is presented in terms of ethnicity, with the Slavic groups operating in the North-eastern regions of the country, where they are involved in money laundering activities and investments, mainly in the real estate sector; while, the Caucasus groups, namely the Georgian clans, are mainly active in the Southern regions, where they are involved in property crime. Then, the case of the Baltic countries (Estonia, Latvia, Lithuania) is a specific one, due to the fact that in these countries the *Rossijskaja Organizacija* must be considered an indigenous problem, rather than and exogenous one. In fact, a large historical community of ethnic Russians is present in Estonia, Latvia and Lithuania, which acts as a facilitating factor for the penetration of Russian organised crime. Moreover, the Baltic countries case study is functional to analyse the money laundering mechanism applied by the *Rossijskaja Organizacija*, which represents the main activity carried out

[4] Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 1st August 2018. Available in German at: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html.

in these countries by Russian criminal networks, as well as to show how Russian organised crime penetrates within the European legal economy.

Moreover, the distinct character, nature and organisation of the *Rossijskaja Organizacija* are considered under the hypothesis sustained in the present research that the *Rossijskaja Organizacija* cannot be ascribed to a mafia-like paradigm, as it is sustained in part of the literature dedicated to the phenomenon, since it lacks the high-degree of centralisation and the tight vertical hierarchical structure of a typical mafia network, it presents rather a fluid nature based on a more horizontal hierarchy. Moreover, the role played by familial ties and ethnicity, which is substantial in shaping the mafia network, are just secondary issues when considering the *Rossijskaja Organizacija*, where the main driver for the creation of a criminal network lies on the shared criminal interest and the mutual benefits thereof, as observed by Finckenauer and Voronin[5]. Furthermore, the main networks of the *Rossijskaja Organizacija* in Europe, their *modus operandi* and characteristics are taken into account. The classification of the Russian criminal networks adopted in the research is that one proposed by Galeotti[6] of two main groups classified according to ethnicity: the Slavic and the Caucasus groups. Among the Slavic groups, the most relevant are the Moscow-based *Solncevskaja Bratva*, the *Tambovskaja Bratva* based in St. Petersburg and the *Uralmaš gruppirovka* of Ekaterinburg. Then, considering the Caucasus groups, the attention has been placed on the loose networks of Georgian and Chechen origins. Specifically, the Georgian groups are analysed in the case study of the *Rossijskaja Organizacija* infiltration in Italy, where are operating the *Kutaisi*, *Tbilisi* and *Rustavi* clans, mainly in the southern region of Apulia, specifically in the city of Bari.

Another relevant aspect taken into consideration in the present thesis is the already mentioned "criminal-governmental nexus", an expression employed in the research to indicate the degree of cohabitation of the Russian state with the organised crime. What is demonstrated is that Russia is employing the *Rossijskaja Organizacija* in Europe as a tool of the Kremlin geopolitical agenda to undermine the West through covert and indirect operations[7]. This linkage is investigated through an analysis of the role played by the Russian security services, particularly the Foreign Intelligence Service (SVR), the Federal Security Service (FSB) and the military intelligence (GRU), notably in the cyber-attacks conducted against Western targets in the context of the Russian doctrine of *Informacionnaja Vojna* ('Information Warfare') and in the use of 'black account' funds (*čërnaja kassa*) to finance political operations conducted in Europe. The cybersecurity domain represents one of the main sectors of activity of the *Rossijskaja Organizacija*, which shows a considerable expertise and sophistication in the operations deployed. A specific focus on cybersecurity and the Russian cyber threat to Europe is discussed in chapter four to highlight the connection between the Russian state and the *Rossijskaja Organizacija*. Cybersecurity represents one of the priority items in the European security agenda, due to a number of factors, among which the continuous technological advancement, the high level of

[5] Finckenauer James O., Voronin Yuri A., *The Threat of Russian Organised Crime*, Issues in International Crime, NCJ 187085, June 2001.
[6] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Heaven and London: Yale University Press, 2018).
[7] Galeotti Mark, *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations, May 2016.

technical expertise characterising the cyberattacks and the growing extension of the phenomenon worldwide, which has registered, over the last three years, an increase of 77.8% in terms of cyberattacks deployed. Moreover, taking into account the Russian case, cyber domain is considered to play a fundamental role in the Information Warfare (IW) strategy, which is interpreted in the Russian political, academic and military discourses as a set of methodologies and techniques employed to gain power and influence the public opinion. The concept of IW has to be interpreted in conjunction with the "global information struggle" as stated by the Russia's National Security Strategy 2020, where a clear opposition with the West is presented. According to the Russian cybersecurity doctrine, cyberwarfare is officially included into the IW and the *Rossijskaja Organizacija*, unofficially, contributes in a relevant way to the IW conducted by the Russian Federation to defend its national interests and pursue its geopolitical goals. In this context, the argument sustained in the present research is that the Kremlin is employing the *Rossijskaja Organizacija*, particularly in the cyber domain, in the wider framework of the confrontation with the West. The level of connivance between the Russian state and cybercrime is clearly visible in the activities of the Advance Persistent Threat (APT) groups attributable to Russia, which are analysed in detail, through the case studies of APT28 and APT29.

The European response to the threat of organised crime is then presented in chapter five, where the European initiatives and polices to tackle the problem are discussed. Specifically, the European Agenda on Security 2015-2020 is taken into consideration, which represents the strategic framework for the implementation of the security measures within the European Union and sets organised crime and cybercrime, along with terrorism and radicalisation, as the main threats to which the European security architecture is exposed. Then, the European Union Policy Cycle to tackle organised and serious international crime is discussed, a four years policy initiative launched for the first time in 2010 to provide a coordinate and more effective response to the threats placed by organised crime. Furthermore, the operations conducted by Europol to counter organised crime, in the framework of Strategy 2020 and the Programming Document 2019-2021, are considered. In addition, the specific measures to counter the problem of the infiltration of organised crime in the European legitimate economy are analysed, specifically the anti-money laundering measures adopted at the European Union level as well as the initiatives launched under the edges of the European Union Cybersecurity Strategy launched in 2013 by the Commission and the European External Action Service (EEAS), which represents the guideline for the European action in the cyber domain. In conclusion, a particular attention is dedicated to the policies which are necessary to counter the infiltration of the *Rossijskaja Organizacja* in Europe and a section is devoted to the specific policy recommendations proposed for the countries analysed as case studies, namely: Germany, Italy and the Baltic countries.

TRANSLITERATION TABLE

The method of transliteration from the Cyrillic script to the Latin script employed in the present thesis is the scientific or scholarly transliteration system. An illustrative table is provided to assist the reading of Russian words transliterated in the text.

Letter	Scientific transliteration	Approximate English equivalent	Examples
А а	a	f**a**ther	дв**а** *dva* "two"
Б б	b	**b**ed	о**б**а *óba* "both"
В в	v	**v**ine	**в**от *vot* "here"
Г г	g	**g**old	**г**од *god* "year"
Д д	d	**d**oor	**д**а *da* "yes"
Е е	e, ye	**ye**s	н**е** *ne* "not"
Ё ё	ë, yo, jo	**yo**ur	**ёж** *yozh* "hedgehog"
Ж ж	zh, ž	plea**s**ure	**ж**ук *zhuk* "beetle"
З з	z	**z**oo	**з**ной *znoy* "heat"
И и	i	pol**i**te	**или** *íli* "or"
Й й	y, i, j	jo**y**	мо**й** *moy* "my, mine"
К к	k	**k**ey	**к**то *kto* "who"
Л л	l	**l**amp	**ли** *li* "whether"
М м	m	**m**ap	**м**еч *mech* "sword"
Н н	n	**n**ot	**н**о *no* "but"

О о	o	m**o**re	**о**н *on* "he"
П п	p	p**icture**	**п**од *pod* "under"
Р р	r	rolled **r**	**р**ека *reká* "river"
С с	s	**s**et	е**с**ли *yésli* "if"
Тт	t	**t**able	**т**о**т** *tot* "that"
У у	u	t**oo**l	**у**же *uzhé* "already"
Ф ф	f	**f**ace	**ф**орма *fórma* "form"
Х х	kh, h, x	lo**ch**	ду**х** *dukh* "spirit"
Ц ц	ts, c	si**ts**	коне**ц** *konéts* "end"
Ч ч	ch, č	**ch**at	**ч**ас *chas* "hour"
Ш ш	sh, š	**sh**arp	ва**ш** *vash* "yours"
Щ щ	shch, šč	**sh**eer	**щ**ека *shcheká* "cheek"
Ъ ъ	″	(called "hard sign") silent, prevents palatalization of the preceding consonant	об**ъ**ект *obyékt* "object"
Ы ы	y	h**i**t	т**ы** *ty* "you"
Ь ь	'	(called "soft sign") silent, palatalizes the preceding consonant	вес**ь** *vyes'* "all"
Э э	è, e	m**e**t	**э**то *èto* "this, that"
Ю ю	yu, ju	**u**se	**ю**г *yug* "south"
Я я	ya, ja	**ya**rd	р**я**д *ryad* "row"

I. ORGANISED CRIME IN EUROPE: CHARACTERISTICS, TRENDS, THREATS

1. Definition of organised crime

The proliferation of criminal activities affects not only security in strict terms, but stability and governance as well. Security should be interpreted in a holistic way, since it encompasses all aspects of society and it involves both the individual and the community levels. Moreover, security can be effectively guaranteed only when requirements such as good governance, transparency, lack of corruption, institutions accountability and confidence in the government are met. Organized crime damages all these fundamental pillars of a democratic country. Furthermore, organized crime is not the same in all the countries, indeed it is diversified and adapts itself to the existing social relations and favourable conditions, showing different degrees of effectiveness and intensity case by case. This means that an adequate way to contrast organised criminal activities is to apply a country-specific filter of analysis. A specific feature of a criminal organisation is the strive for power and social prestige, acquired through infiltration into the public and business sectors. Moreover, organised criminal organisations are characterised by a high degree of managerial structure, professionalism, tight hierarchy, division of tasks and sometimes a code of honour based on familial ties or clan values.

The United Nations Convention on Transnational Organized Crime (UNTOC) defines organised crime in article 2(a) as: " […] a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit".[8]

Transnational organised crime (TNOC) presents the same elements of organised crime mentioned above with a distinction though, it is not limited to a country, but it is grounded on the coordination of criminal activities across national borders, involving networks planning and executing illegal business ventures in more than one country. Nevertheless, the aforementioned convention contains no precise definition of "organised crime" or "transnational organised crime", since there is no consensus, both in practice and in theory, on a definition of the concepts, due to the continuously evolving and expanding nature of criminal activities, at the local and global levels.

The present research embraces the definition of organised crime provided by Varese[9], that considers organised crime as a form of governance. In particular, the Italian scholar distinguishes between corporate governance – the way in which a corporation is managed and how it handles the relations externally – and economic governance, referring to the rules regulating the exchanges. In this view Varese asserts that "an organised crime group attempts to regulate and control the production and distribution of a given commodity or service

[8] United Nations – General Assembly, *United Nations Convention on Transnational Organized Crime (UNTOC)*, RES. 55/25, 15th November 2000. Available at: https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf.

[9] Varese Federico, "What is Organized Crime?" in F. Varese (ed.), *Organized Crime: Critical Concepts in Criminology*, (London: Routledge, 2010).

unlawfully".[10] According to this definition, an organised crime group necessitates of a range of resources to achieve its goals, among which the most relevant is violence. As a matter of fact, to impose a hegemonic control over a given market sector, a group must be stronger than others to be respected. Another fundamental resource consists in the knowledge about the scenario in which the group is operating, namely information. A third compulsory resource to be owned in order to establish an organised crime group is governance, the structure, the system upon which relies all the members, which issues the orders and grants rewards. Organised crime is therefore a form of governance, as well as mafia groups and the State itself, according to Varese. The Italian scholar proposes a categorisation, according to which all the three aforementioned entities – organised crime, mafia and the State – belong to the same category, that one of governance, due to the fact that all of them share the same aspiration, that one of governing exchanges and of imposing a hegemonic control over them. Therefore, it is useful to analyse the other entities mentioned, namely the mafia and the State. When defining mafia, Varese affirms that is "a type of organised crime group that attempts to control the supply of protection"[11]. Both organised crime and mafia groups compete with the State in offering services of governance. The State in fact "uses violence to protect assets and enforces agreements (contracts) among individuals, and a territory where these individuals reside demarcated by reach of the enforcer's enforcement power".[12] Both organised crime group and mafia attempt to govern a given domain, to impose their hegemony and to acquire power, what distinguishes an organised crime group from a mafia group is the fact that the latter does not limit its action to just one market sector but it controls several markets and, more importantly, it constantly challenge the State, in the attempt to substitute it. Moreover, the ties and the hierarchy in a mafia group are far more relevant than in a common organised crime group. Mafia is a pervasive and all-encompassing system, which permeates a territory and the relations among the individuals in that given territory, either being them part of a mafia group or not. Besides the categorisation of mafia as "organised crime group", other characterisations have been developed through history, according to different models of interpretation, either as a "secret society" and the consequent features or as a "behaviour" and as a "enterprise"[13]. Regardless of the categorisation that is applied, what is relevant is to underline the fact that the mafia is something more complex than a common organised group, with broader aims and aspirations, and with a higher degree of structural organisation and well deep-rooted ties among the members. Nevertheless, both organised crime groups and mafia share one objective, that one of governance and the challenge to the State, that can turn into open confrontation or cohabitation, giving birth in the latter case, to a hybrid entity where the divide between legal and illegal activities becomes blurred. The case that is analysed in the present research, the *Rossijskaja Organizacija*, falls under that category, that one of the cohabitation with the State.

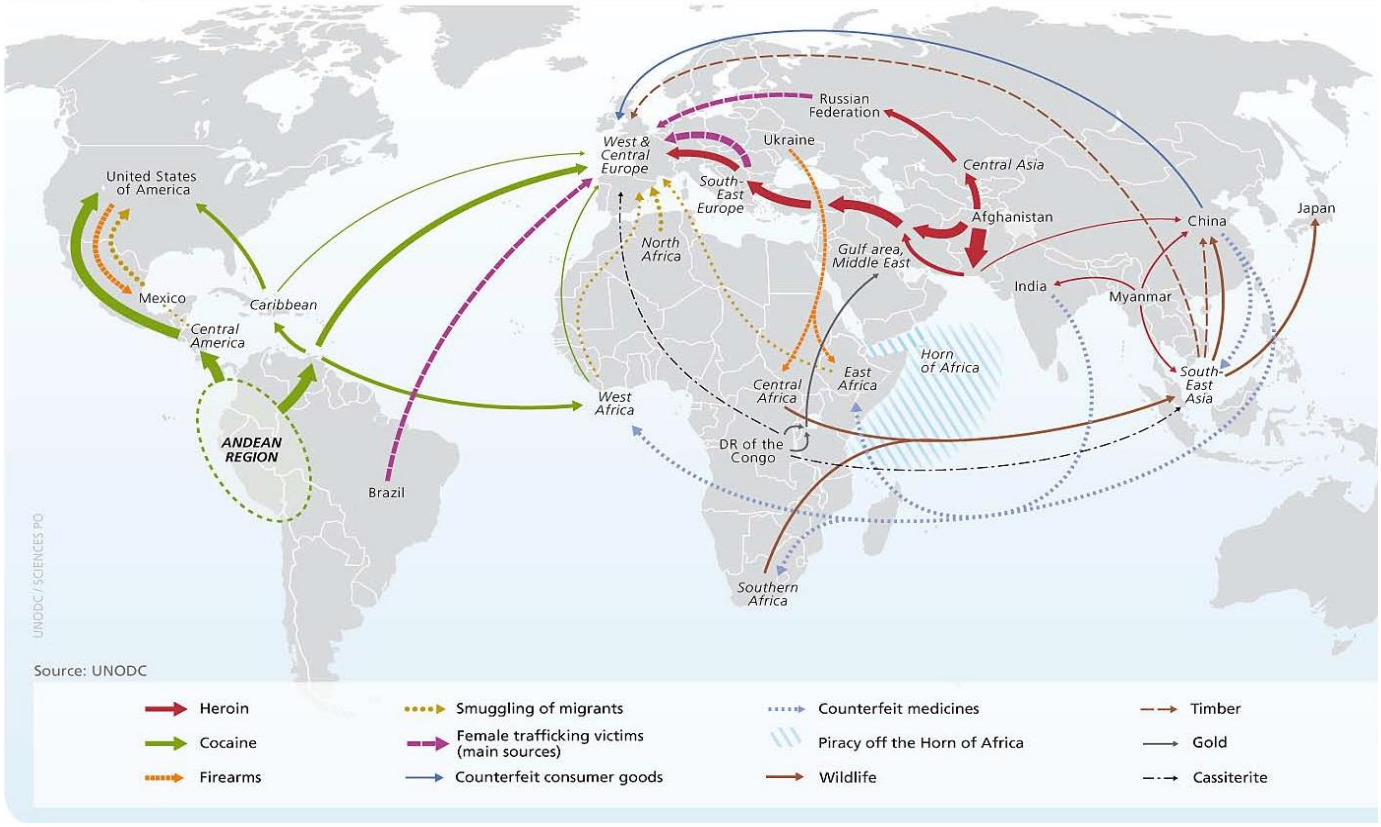
[10] Ibidem.
[11] Ibidem.
[12] Ibidem.
[13] For further information on mafia's models of interpretation see: Paoli Letizia, "Organised Crime in Italy: Mafia and Illegal Markets – Exception and Normality", in Fijnaut C., Paoli L. (eds) *Organised Crime in Europe*. Studies of Organized Crime, Vol 4, (Dordrecht: Springer, 2004), pp. 263-302.

2. Contemporary outlook of organised crime in Europe

To tackle the problem represented by organised crime, it is necessary to focus not only on the groups but also on the activities carried out by them. Organised crime and, more broadly, transnational organised crime, focus on a wide range of illicit activities, among which: currency counterfeiting; cybercrime (e.g. child sexual exploitation, cyber-dependent crimes; payment card fraud); drug production, trafficking and distribution; fraud (e.g. excise fraud, investment fraud, mass marketing fraud, payment order fraud, value added tax fraud); illicit waste trafficking; intellectual property crime; migrant smuggling; organised property crime; sports corruption; trafficking of endangered species; trafficking of firearms and trafficking in human beings.

It is relevant to adopt a view centred on the criminal activities rather than on groups, since even if the perpetrators of a given crime are arrested and incarcerated, the activities continue since the derived profits and the illicit market remain. Therefore, as asserted by the United Nations Office on Drugs and Crime's analysis, "strategies aimed at the groups will not stop the illicit activities if the dynamics of the market remained unaddressed".[14] Organised crime poses a huge threat to the world economy and governance, in terms of the

Fig.1 Flows of transnational organised crime activities at the global level



Source: UNODC, The Globalization of Crime. A transnational Organized Crime Threat Assessment, 2010.

[14] UNODC, *The Globalization of Crime. A transnational Organized Crime Threat Assessment*, 2010. Available at: https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf.

damages directly caused by specific forms of crime and of the indirect impact of the crime activities on the authority of a state and its governance.

3. Main characteristics of organised crime in Europe

Organised crime groups (OCGs) operating in the European Union (EU) present different forms, from traditional OCGs to smaller criminal networks. According to the data provided by the Europol 2017 Serious and Organised Crime Threat Assessment (SOCTA)[15], there are more than 5.000 international OCGs currently under investigation, belonging to more than 180 different nationalities. OCGs in the EU are not attributable to just one structural model, most of them are hierarchically organised but just 30-40% of them consists of loose networks, while 20% exists just for a short period of time. As far as the composition is concerned, as reported by SOCTA 2017, 76% of OCGs are made of six or more members and only 24% of them are composed by up to five members. Moreover, 60% of the suspects involved in organised criminal activities in the EU are EU nationals. Taking in consideration the activities, what emerges is that production, trafficking and distribution of drugs remain the key criminal activity in the EU, accounting for more than one third of the OCGs operations. Other main criminal activities are organised property crime, migrant smuggling, trafficking in human beings and fraud. Moreover, the main trend underlined by SOCTA 2017 report is the poly-criminality, a feature characterising OCGs groups in the EU, with 45% of them typically active in more than three countries. This trend is determined by a number of factors, among which the technological progress (e.g. the impressive expansion of the online trade in illicit goods and services). Furthermore, on the one hand OCGs groups are adapting to new market models such as the supply chain, while on the other, new concepts have been developed such as that one of Crime-as-a-Service (CaaS), which consists of specific criminal ventures created by individual criminal entrepreneurs on *ad hoc* basis. The technological advancement determines also other effects, among which the facilitation of corruption methodologies by means of online services. In fact, some OCGs employ new payment methods, such as cryptocurrencies, online payments and alternative banking platforms to transfer funds to corrupted individuals in the public and private sectors, which makes it more difficult to uncover corruption. Furthermore, online platforms and applications are not subjected to the same level of regulation of traditional financial service providers. This lack of regulation creates optimal conditions for money-laundering, which contributes to the growth of the criminal markets in the EU. There are two main methods of money laundering, the first and most used one involves cash smuggling by couriers or using post and parcel services, while a second method is the so-called trade-based money laundering, which consists in using false invoicing and forged ID documents used by OCGs' shell companies to cover criminal funds and money transfers. As far as the online trade in illicit goods and services is concerned, it is worth mentioning

[15] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017. Available at: https://www.europol.europa.eu/socta/2017/.

that according to the data provided by Europol[16], it is expected to grow in a relevant and rapid way in the next years. Moreover, online platforms will emerge as the key distribution platforms for all types of illicit goods in the EU. At the present moment the Darknet[17] is the main platform employed by OCGs, offering different markets and hidden services. An example is the illegal firearms selling through the use of Darknet marketplaces in Slovenia, as detected by the Slovenian law enforcement authorities and Europol in December 2016[18]. Another relevant aspect, when discussing OCGs' activities, is that one related to the vulnerabilities and the facilitating factors which can be exploited by criminals. For instance, the continuous technological advancement, that, while producing beneficial effects for the economy and the society, is creating new vulnerabilities as well. In fact, OCGs in Europe show a high degree of adaptability to changing technological scenarios and high level of efficiency in exploiting new vulnerabilities. The Internet and the increasing connectivity (e.g. the 5G transition) will expand the Internet of Things (IoT), thus increasing the number of connected devices susceptible of malicious intrusion by cybercriminals. Another element which represents a driver for organised criminal activity in Europe is represented by the changing geopolitical context. The impact of conflicts, such as the Libyan and the Syrian ones, can be seen in the steady migration flows towards the EU and in the increase of revenues for the associated migrant smugglers or in the growth of the illegal firearms market originating in these countries.

In the following sections will be discussed the main criminal activities conducted in the EU, namely: drug trafficking, human trafficking and migrants smuggling, illegal trafficking of firearms; money laundering; cybercrime (to which an entire section of the present research has been dedicated in chapter four).

4. Sectors of activity in the illicit market

4.1. Illegal Drug trafficking

Illegal production and trafficking of narcotics is one of the most prominent form of modern organised crime and a serious threat to the European security. As reported by SOCTA 2017, more than one third of the OCGs active in the EU are involved in the production, trafficking or distribution of drugs[19]. It is estimated that in the

[16] Ibidem.

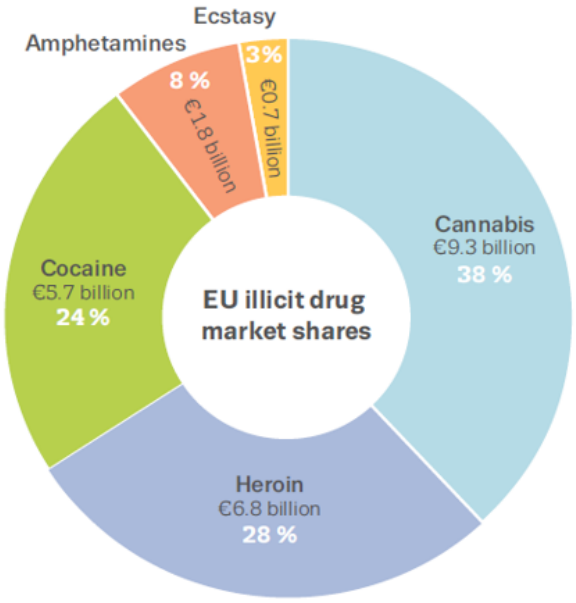
[17] The *Darknet* is a decentralised and anonymous network, within the deep web, that is not indexed by common search engines (e.g. Google) and that can only be assessed using specific software such as The Onion Router (TOR), I2P and Freenet. The Darknet is associated with the encrypted part of the Internet (Tor network), where illicit trading takes place (e.g. the online drug bazaar Silk Road). However, the Darknet is not only employed for illicit selling of goods, but also for anonymous communication between whistle-blowers, journalists through use of applications such as SecureDrop.
The *Deep web* refers to any internet information or data that is inaccessible by a search engine and includes all web pages, websites, intranets, networks and online communities that are intentionally and/or unintentionally hidden. The opposite term to the deep web is the *surface web*, which is accessible to anyone using the Internet.

[18] Europol – Press Release, *Darknet Arms Vendor Arrested in Slovenia with Support of Europol*, 20th December 2016. Available at: https://www.europol.europa.eu/newsroom/news/darknet-arms-vendor-arrested-in-solvenia-support-of-europol.

[19] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.

European Union alone, the illicit drug market generates about €24 billion euros in profits per year[20]. Illicit drug market, supplied both by domestically cultivated and manufactured drugs and drugs trafficked into Europe from outside, represents the most lucrative criminal activity in the European Union. According to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)[21], the largest profit of the EU illicit drug market shares comes from the cannabis (€9.3 billion euros), followed by heroin (€6.8 billion euros), cocaine (€5.7 billion euros), amphetamines (€1.8 billion euros) and ecstasy (€0.7 billion euros). The market for cannabis results to be the largest drug market in the EU, where it is distributed as cannabis resin and herbal cannabis. The main source of herbal cannabis is Albania, while Morocco is the main country of origin for resin cannabis, which is smuggled from Libya to the EU across the Mediterranean Sea. Considering cocaine, what is relevant to mention in relation to the European context is that the main entry points are Belgium, Spain and the Netherlands, while the main producers are Colombia, Perú and Bolivia. Relevant considerations, when analysing the European security, can be made for trafficking of heroin and synthetic drugs and new psychoactive substances (NPS). Considering the heroin market, the channel allowing the realisation of the aforementioned profits (€6.8 billion euros) relies on the existence of the so-called Balkan Route, on which opioid drugs are trafficked from their original production sites in Afghanistan, Pakistan and the Islamic Republic of Iran, and transit through Turkey and the Balkans onward to Central and Western Europe. Diamorphine, also known as heroin, is one of the main opioids trafficked through the Balkan Route. According to UNODC last estimates[22], total global opium production jumped by 65% from 2016 to 2017, to 10.500 tons, the highest estimate ever recorded by UNODC. Of the 10.500 tons of opium produced worldwide in 2017, it is estimated that some 1.100–1.400 tons remained unprocessed for consumption as opium, while the rest was processed into heroin, resulting in an estimate of between 700 and 1.050 tons of heroin manufactured worldwide, 550–900 tons of which were manufactured in Afghanistan. As a matter of fact, it is worth mentioning that the surge in the worldwide opium production was highly influenced by Afghanistan, which

Fig.2 Estimated minimum retail value of the illicit market for the main drugs in the EU



Source: EMCDDA, *European Drug Report 2018: Trends and Developments*, June 2018.

[20] United Nations, International Narcotics Control Board, "Chapter III: Analysis of the World Situation" in *Report 2017*, January 2018. Available at: https://www.incb.org/documents/Publications/AnnualReports/AR2017/Annual_Report/E_2017_AR_ebook.pdf.

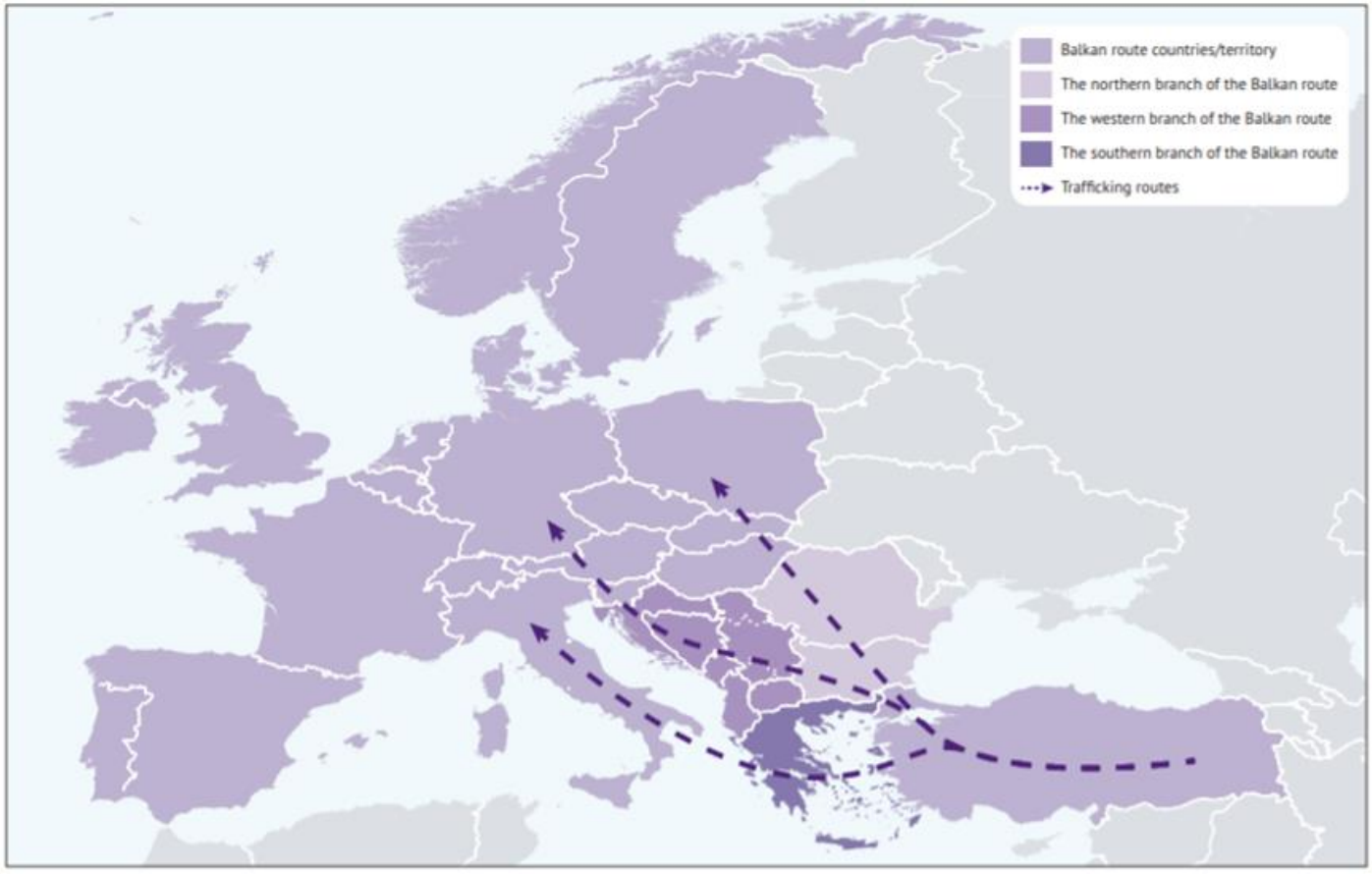
[21] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *European Drug Report 2018: Trends and Developments*, June 2018. Available at: http://www.emcdda.europa.eu/publications/edr/trends-developments/2018.

[22] United Nations Office on Drugs and Crime (UNODC), *World Drug Report*, 2018. Available at: https://www.unodc.org/wdr2018/.

registered in 2017 an increase of 87% from the previous year, reaching a total value of 9.000 tons. Europe has been a lucrative market for traffics of Afghan heroin for more than twenty years. According to recent data elaborated by the UNODC, the total value of illicitly trafficked heroin and opium to Western Europe through the Balkans is registered at some US$ 28 billion per year, and this estimate pertains only to opiates trafficked along the Balkan route and does not consider other relevant routes such as the Northern route to Central Asia and Russia.[23] Moreover, as underlined by the United Nations International Narcotics Control Board (INCB), the involvement of Balkan criminal organised groups in the market has seen a further increase in the last years.[24]

Furthermore, the Balkan route, is divided in several minor branches, among which the "Classic Route", which begins in Turkey and goes through Bulgaria, Macedonia, Kosovo, Serbia, Bosnia and Croatia, towards the European Union; the "Northern Route", which also begins in Turkey and goes through the Black Sea and Ukraine or Bulgaria, Romania, Hungary, towards Austria and Slovakia; and the "Southern Route", passing through Greece, Macedonia and Albania to Italy. Moreover, as pointed out by the European Monitoring Centre

Fig.3 The three branches of the Balkan route through South-Eastern Europe



Source: UNODC, *Drug Money: the illicit proceeds of opiates trafficked on the Balkan route*, 2015.

[23] UNODC (2015), *Drug Money: the illicit proceeds of opiates trafficked on the Balkan route*. Available at: https://www.unodc.org/documents/data-and-analysis/Studies/IFF_report_2015_final_web.pdf.
[24] United Nations, International Narcotics Control Board, *Report 2017*, January 2018. Available at: https://www.incb.org/documents/Publications/AnnualReports/AR2018/Annual_Report/Annual_Report_2018_E_.pdf.

for Drug and Drug Addiction (EMCDDA) in its analysis of 2018[25], heroin is the most common opioid in the EU drug market. According to the report, between 2002 and 2014, the quantity of heroin seized within the European Union accounts for a range value from 5 to 10 tonnes, and has stabilised in recent years, with 4.3 tonnes registered in 2016.

The second drug market particularly relevant for the European security is represented by that one of the synthetic drugs and new psychoactive substances (NPS). This drug market involves different countries of the EU and most notably, Belgium and the Netherlands, which are globally one of the main production and distribution hubs for 3,4-methylenedioxymethamphetamine (MDMA), amphetamine. According to the analysis of Europol[26], the market of synthetic drugs is the most dynamic of the drug markets in the EU and new production sites are expected to appear in other Member States of the EU. Moreover, a significant increase of production capacity of synthetic drugs has been registered in the recent years and new NPS are continuously produced, as testified by the 419 new NPS detected in the EU over a period from 2012 and 2017[27].

These data clearly show that the drugs market in Europe is a growing problem that affects the security of the region. Another aspect that must be considered is that one concerning drug-related harms in the health domain – being drug consumption recognised as a major contributor of the global burden of disease – that, as a consequence, determine high public expenditure devoted to medical treatments, structures, rehabilitation centres and measures of social providence. A second aspect, more relevant for the present paper, is related to the harm caused to the State structure. Economic resources generated by the illicit trafficking of drugs are used for destabilizing the society, the political system, the administration and the economy of a country in several ways, through: the creation of "grey zones" where no law enforcement is possible; the erosion of confidence in the market; an increased volatility of the aggregates in a country's financial system; a distortion of the economic database and hampering of the economic policymaking; the spread of corruption in national security.

4.2. Migrant smuggling

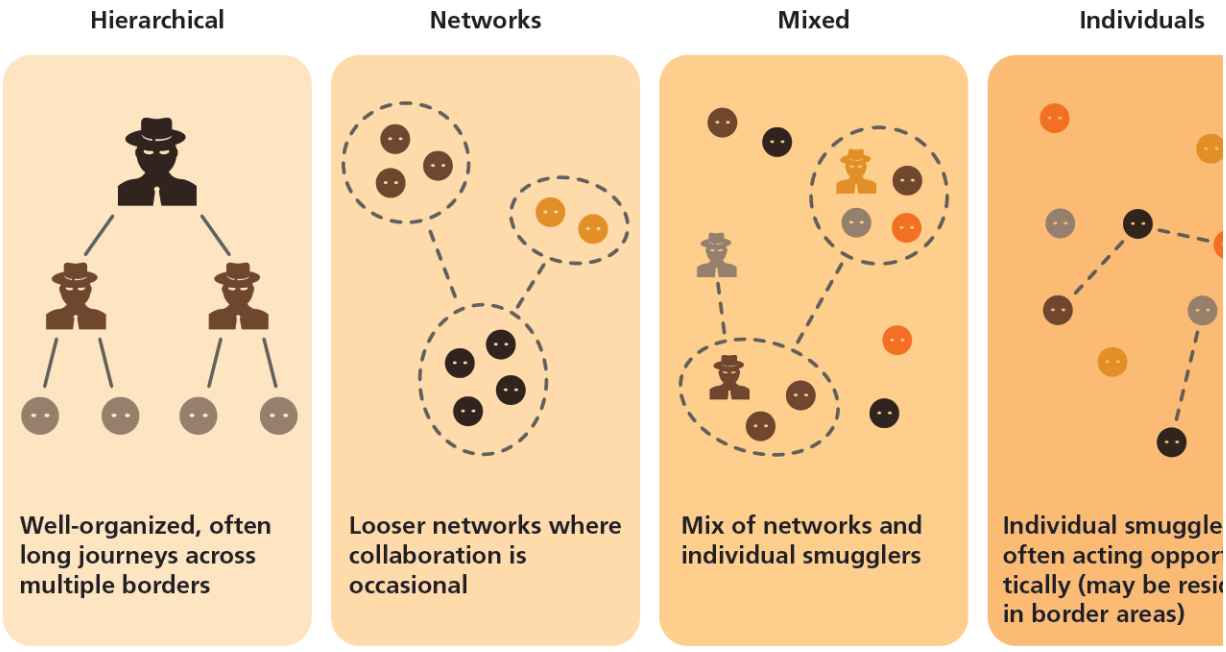
Another market that generates profits comparable to the drugs market is that one related to migrant smuggling, which has registered a significant increase since 2015, with the European migrant crisis, also known as the refugee crisis, characterised by high numbers of people arriving in the EU from across the Mediterranean Sea. Nevertheless, a decrease in this trend has been registered in 2017, with the number of people crossing EU borders illegally falling from 1.8 million in 2015 to 204.219 in 2017[28]. The European Asylum Support Office (EASO) reported that, during 2018, 634.700 applications for international protection were lodged in the EU,

[25] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *European Drug Report 2018: Trends and Developments*, Publications Office of the European Union, Luxembourg, 2018, p.23.
[26] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
[27] Ibidem.
[28]FRONTEX, *Risk Analysis for 2018*, Warsaw, 2018. Available at: https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_for_2018.pdf.

a 10% decrease from 2017[29]. Consequently, the EU countries issued about 593.500 decisions in first instance, of which 34% (201.790) were granting EU-regulated protection, mostly refugee status[30]. This means that a potential number of irregular migrants (391.710), whose applications were rejected, may have attempted to stay in the EU.

According to the data provided by Europol[31], in 2015 migrant smuggling in the EU produced profits equal to an estimated €4.7 to 5.7 billion euros. The OCGs dealing with migrant smuggling present a high degree of organisation and coordination and most of the perpetrators are citizens of the countries of departures, while a minority are based in destination countries. Moreover, according to UNODC[32], OCGs involved in migrant smuggling present different configurations in terms of structure. In particular, four main organisational models have been detected: the hierarchical model characterises OCGs which deploy large scale operations, benefiting from transnational links and developing a sophisticated process, involving the use of counterfeit or fraudulently obtained travel documents; a second model is represented by the loose networks, where the members act with more autonomy in different stages of the smuggling process (e.g. counterfeiting documents, facilitating a specific border crossing); then, individual smugglers as well have been identified, which offer low-level services in specific border or transit areas; finally, there is a mixed model, which combines the different elements of the aforementioned structures, according to the changing contexts and necessities.

Fig.4 Migrant smuggling: OCGs' organisational models



Source: UNODC, *Global Study on Smuggling of Migrants*, 2018.

[29] EASO, *EU+ asylum trends 2018 overview*, February 2019. Available at: https://www.easo.europa.eu/sites/default/files/EASO-2018-EU-Asylum-Trends-Overview.pdf.
[30] Ibidem.
[31] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA)*, 2017.
[32] UNODC, *Global Study on Smuggling of Migrants 2018*, June 2018. Available at: https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf.

There are several smuggling routes towards Europe, among which the major ones are represented by: the Central Mediterranean route, whose departure point is North Africa (mainly from Libya) and whose arrival point is Italy (mainly Sicily); the Eastern Mediterranean route from the Turkish coast to several Greek islands, and the Western Mediterranean route from Morocco to Spain. Other routes, with different extent of smuggling activities, have been traced across the European continent. Migrant smuggling happens also along the European Union's Eastern border (6.000 km), which includes part of the Eastern borders of Norway, Finland, Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Bulgaria and Romania. An alternative path is that one represented by the Black Sea route, through which migrants are smuggled from Turkey to Romania and Bulgaria. Migrant smuggling has also been registered within Europe, by means of the so-called Western Balkans route, from Greece and Bulgaria directed towards Hungary, Croatia or Romania.

In order to combat migrant smuggling the European Migrant Smuggling Centre (EMSC) was set up in February 2016 to support the investigations conducted by Member States of the EU and to improve cooperation and coordination among law enforcement agencies. The EMSC is conceived as a centre of expertise and information hub on migrant smuggling and human trafficking intelligence and it provides support to EU law enforcement agencies on a weekly basis, providing strategic intelligence reports on migrant smuggling trends and *modus operandi*. According to the EMSC's 3rd Annual Activity Report[33], the migratory pressure from Africa is likely to continue to have an impact on migrant smuggling routes towards the EU. Moreover, technological progress acts as a facilitator for OCGs, which will increasingly employ anonymising technologies such as burner apps or hard-to-trace phone numbers, thus impeding the tracing or monitoring of criminals by law enforcement agencies.

Furthermore, due to the measures enacted by the EU, the number of irregular migrant arrivals to the EU has decreased, reaching the lowest level in five years (144.166 in 2018)[34]. Nevertheless, the threat of criminality at the external borders remains significant, with several irregular migrants trying to illegally cross the EU borders each year and a huge quantity of them smuggled in secondary movements or involved in trafficking-related crimes.

4.3. Trafficking in human beings

The European migration crisis has resulted in an increase in the number of potential victims of trafficking in human beings (THB). According to the analysis of the European Commission[35], on the data collected from 2015 to 2016 in the EU28, 44% of the registered victims of trafficking were citizens of EU Member States

[33] Europol – European Migrant Smuggling Centre (EMSC), *3rd Annual Activity Report 2018*, 2019. Available at: https://www.europol.europa.eu/publications-documents/emsc-3rd-annual-activity-report-%E2%80%93-2018.

[34] European Commission, *European agenda on migration*, Brussels, 2015. Available at: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-migration_en.

[35] European Commission, *EU Data collection on trafficking in human beings in the EU*, Brussels, 2018. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181204_data-collection-study.pdf.

and 56% were non-EU citizens. The top five EU countries of citizenship of those victims were Romania, Hungary, the Netherlands, Poland and Bulgaria. On the other hand, the top non-EU countries of citizenship of the victims were Nigeria, Albania, Vietnam, China, and Eritrea. These data are particularly relevant, since they highlight that THB is an issue related not only to the external borders of the EU.

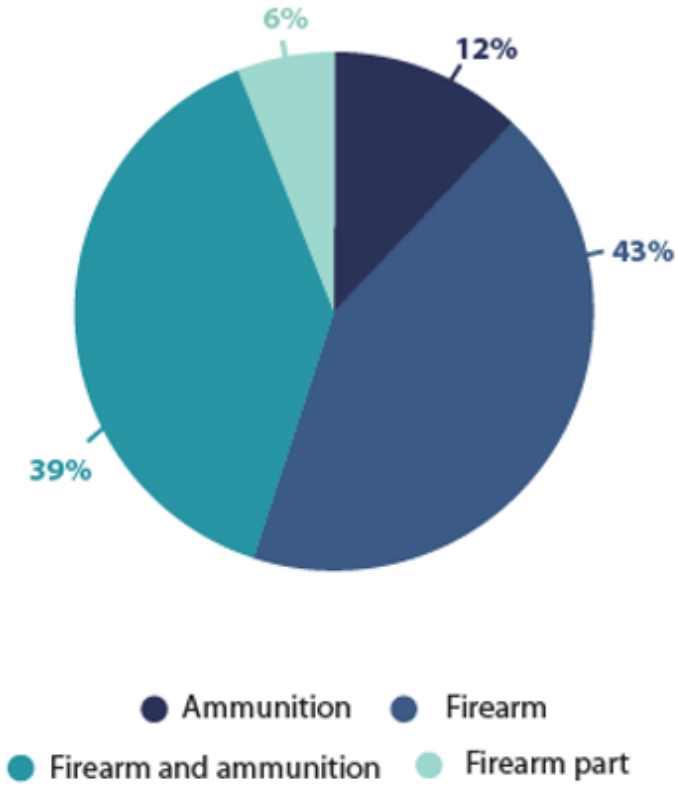
Considering the different forms of THB, sexual exploitation is the most common, covering over half (56%) of the cases registered, while labour exploitation accounts for around one quarter (22%). Other forms were employed for the remaining cases registered (18%). The five Member States with the highest percentage of victims of sexual exploitation in 2015-2016 were: Slovenia (97%), Hungary (96%), Estonia (83%), Croatia (76%), and Denmark (76%). On the other hand, the five Member States with the highest percentage of victims of labour exploitation were: Malta (84%), Portugal (73%), Czech Republic (56%), Belgium (52%), and the United Kingdom (46%). Considering data according to gender and age, what emerges is that over two-thirds (68%) of registered victims of THB in the period 2015-2016 were females and that almost one quarter (23%) were individuals below eighteen years old.

Considering the citizenship of the traffickers, the top five Member States with the highest number of reported persons suspected, arrested or cautioned for THB were: Romania, Germany, Czech Republic, Bulgaria, and France in 2015-2016 according to the aforementioned data of the European Commission[36].

If the *modus operandi* is taken into account, as far as the sexual exploitation is concerned, a different methodology has been observed whether the victims are EU nationals or not. Sexual exploitation of the former group does not longer rely on the use of violence and coercion, rather most of OCGs employ the threat of violence towards the victims or their family. On the other hand, victims of non-EU countries are predominantly subjected to violence and form of coercion[37]. Moreover, the Europol has confirmed the general trend of OCGs increasing use of legal businesses, which disguise exploitation such as hotels and nightclubs[38]. As far as the *modus operandi* of THB for labour exploitation is considered, traffickers continue to target less regulated industrial sectors (e.g. agriculture, cleaning, construction, entertainment, fishing, retail and transportation) and those requiring season workers in general. Furthermore, the involvement of OCGs in THB for labour exploitation in the EU is expected to increase, which places it as a priority for the European security agenda. In addition, it is worth mentioning the link existing between migrant smuggling and trafficking in human beings. In fact, there are evidences, according to which OCGs involved in THB take advantage of the migrant smuggling routes within the EU.

[36] Ibidem.
[37] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
[38] Ibidem.

Fig.5 Types of firearms seized in the EU (2010-2015)



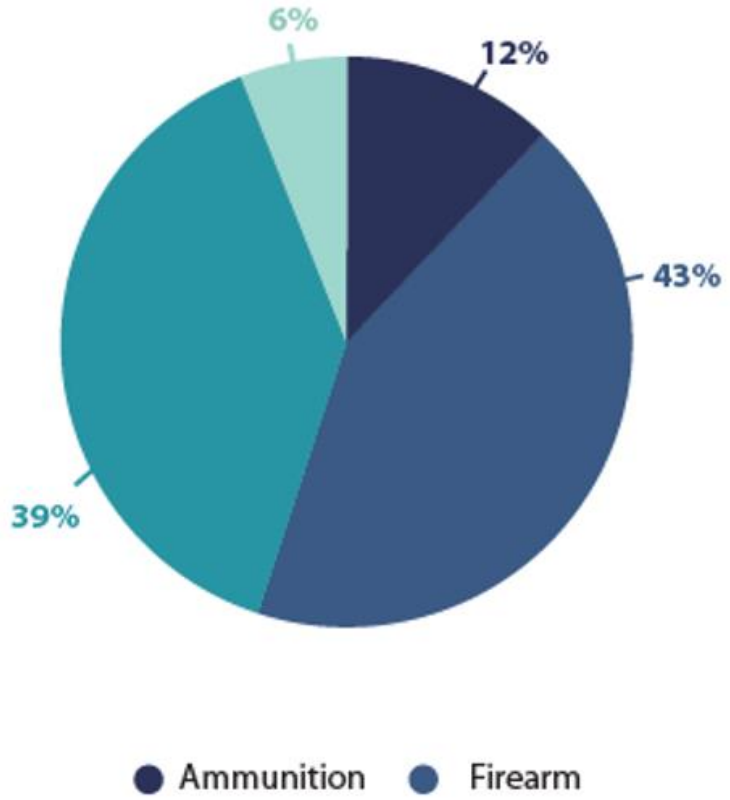
Source: Transcrime – Final Report of Project FIRE, *Fighting lllicit Firearms Trafficking Routes and Actors at European Level*, 2017.

Illicit trafficking of firearms is recognised as a priority on the European agenda particularly since 2016, when it was found to support terrorist activities. As a matter of fact, the EU is revising the Firearms directive[39], to efficiently fight organised crime and terrorism. A specific characteristic is that, unlike other illicitly trafficked goods, firearms are durable, this means that they can circulate for decades and be sold repeatedly. Control over the licit market of firearms and traceability is fundamental, since the evidences show that illicit trafficking of firearms generates through diversion from the licit market. Licit firearms can be diverted for instance by leakage from surplus stocks, theft from stockpiles or individuals or by means of conversion. Conversion of licit firearms to illicit ones is one of the most common methods, it can be applied through reactivation of deactivated firearms, modification of semi-automatic firearms into automatic ones, conversion of blank-firing firearms or replicas. The research conducted by the "Fighting Illicit firearms trafficking Routes and actors at European level" (FIRE) project reported two recent cases of reactivation of deactivated firearms involving Italian OCGs, in particular the 'Ndrangheta and Cosa Nostra[40]. As for the first case, illicit deactivated firearms were bought by 'Ndrangheta in Slovakia, where reactivation standards for firearms are less restrictive than in Italy and then trafficked in Italy. The second case, involving Cosa Nostra, consisted in the illicit trafficking of 151 reactivated firearms (sub-machines, rifles, pistols, revolvers and ammunition),

[39] The Directive 91/477/EEC defines a set of common minimum rules for the control of the acquisition and possession of firearms in the EU, as well as the transfer of firearms to another EU country. This directive was revised first in 2008 by Directive 2008/51/EC and then in 2017 by Directive 2017/853/EC. The 2017 revision, applicable since autumn 2018, brings substantial improvements to security by making it harder to legally acquire certain high capacity weapons, strengthening cooperation between EU countries, and improving the traceability of firearms to reduce the risk of diversion into illegal markets. Text of the directive available at: https://ec.europa.eu/growth/sectors/firearms_en.

[40] Savona Ernesto U. and Mancuso Marina (Eds.). 2017. *Fighting lllicit Firearms Trafficking Routes and Actors at European Level*. Final Report of Project FIRE, (Milano: Transcrime – Università Cattolica del Sacro Cuore, 2017). Available at: www.fireproject.eu.

Fig.6 Types of firearms-related offers on the dark web



Source: Transcrime – Final Report of Project FIRE, *Fighting lllicit Firearms Trafficking Routes and Actors at European Level*, 2017.

bought from an online shop in Slovakia as deactivated firearms and then imported in Italy (Catania, Sicily), where the reactivation process took place. Once reactivated, the firearms were transferred to Malta by plane and to other Italian regions via parcel services. According to the data provided by the FIRE project[41], the seizures of illicit firearms, based on the analysis of 3.875 cases that occurred between 2010 and 2015 in the EU, account for a total of 19.246 firearms, mainly pistols (34%) and rifles (27%).

The regions where most of the seizures took place are Western Europe (35%), Southern Europe (26%), Northern Europe (21%), and Eastern Europe (18%). Within the EU the main destination countries for firearms trafficking are: France, Germany, Greece, Ireland, Italy, the Netherlands, the Scandinavian countries, Spain and the United Kingdom. Main origin countries are the Balkans and countries in the post-Soviet space. Moreover, the recent conflicts close to the EU, for instance the on-going conflict in Eastern Ukraine or in the Middle East and North Africa (MENA), place a threat to the European security system, opening new routes for the illicit firearms trafficking towards the EU. Considering the actors involved in the trafficking, what emerges is that both the supply and demand are dominated by males and the average age of actors generally ranges from twenty to twenty-four years old. Furthermore, the trafficking involves not only OCGs but also corrupted officials and amateurs. As pointed out by the FIRE project analysis, particular attention should be placed in the EU on darknet marketplaces as a source of illicit firearms, as demonstrated by a recent case of high-profile shooting at Olympia-Einkaufszentrum (OEZ) in Munich, where in July 2016 ten people, including the perpetrator, were killed and thirty-six others were injured. From the investigation resulted that the shooter had used an unlicensed deactivated pistol bought on the dark web, reactivated before the mass shooting. The illicit firearms trafficking by means of online market platforms, such as the dark web, should be considered an emerging threat due to the fact that they act as facilitators of firearms trafficking,

[41] Ibidem.

guaranteeing anonymity and concealed identity both to sellers and buyers. Example of online illicit markets are the Armory, Middle Heart, Euroguns, UK guns and ammostore and Nucleus.

4.5. Cyber-dependent crimes

Another significant threat on the European security is that one of the cyber-dependent crimes, which are defined by Europol as "any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)."[42] As far as the society is expected to become increasingly more digitised, cybercrime continues to grow and represents a relevant security challenge. As reported by the Europol 2017 Serious and Organised Crime Threat Assessment[43], organised crime groups operating in the EU are mostly involved in the following activities: Crime-as-a-Service (CaaS); development of malware and cryptoware; network attacks; identity theft; payment order fraud; payment card fraud and online sexual exploitation.

Crime-as-a-Service (CaaS) is defined by Giustozzi, member of the Permanent Stakeholders' Group of the European Union Agency for Cybersecurity (ENISA), as " customerization of cybercrime" including " […] a broad and well-structured offering portfolio ranging from the development of custom malware […] to the massive deployment of attack vector through 'satisfaction guaranteed' spam campaigns based on millions of real and reliable email addresses."[44] The threat stemming from the CaaS is related to the fact that potentially it lowers the cybercrime's entry-barriers, allowing people without IT-expertise to deploy cyber-attacks. CaaS is essentially a model, through which each cybercriminal product and service can be commercialised and sold. CaaS offers all the necessary digital resources to engage in cybercriminal activities, such as malicious software (malware), botnets (infected networks) and stolen databases of personal information.

Another security threat posed by OCGs operating in Europe is that one of the development of malware, malicious software (e.g. virus, worms, spyware, trojans, ransomware), designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is the most frequently encountered cyberthreat, involved in 30% of all data breach incidents reported[45]. Moreover, since 2013, the leading malware in terms of threat and impact is registered to be the cryptoware, which is a ransomware using encryption, whose attack consists in denying access to a victim's files or locking a victim's computer or mobile device, unless a payment is made to regain control of the data and/or devices. As reported by Europol[46], European law enforcement authorities have detected a wide range of ransomware families, among which:

---

[42] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2018. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
[43] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
[44] Giustozzi Corrado, *Commentary: Cybercrime as a service*, Istituto per gli studi di politica internazionale (ISPI), July 2018. Available at: https://www.ispionline.it/en/pubblicazione/cybercrime-service-20979.
[45] Forcepoint, *What is Malware? Malware Defined, Explained, and Explored*. Available at: https://www.forcepoint.com/cyber-edu/malware.
[46] EUROPOL, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.

Cryptolocker, Crysis, Curve-Tor-Bitcoin Locker (CTB-Locker), Dharma and Locky. What is also worth mentioning is the evolution of the cryptoware threat to the European security through the years. In 2014 sporadic cases of cryptoware were registered, while by 2017 the number of ransomware families had notably increased, becoming the most relevant malware threats. The other activity in which OCGs resulted to be prolific in the EU is the deployment of network attacks, which consist in unlawful access to confidential data (i.e. data breaches) or intellectual property. Network attacks can be "active", when the attacker attempts to break into the system, while an attack is defined "passive" when the intruder intercepts communications or monitor other aspects of the network or its devices.

Examples of active attacks are the following:

- *fabrication*: when a false routing message is generated, causing incorrect information about the route between devices;
- *modification*: alteration of the routing transmission to cause delay in the sender and receiver's communication;
- *denial of services*: is an attack whose aim is to shut down a machine or network. The means employed consist of flooding the target with traffic or sending to it information that triggers a crash[47];
- *sinkhole*: it is a service attack that precludes to the base station the availability of complete and correct information;
- *spoofing*: it consists of disguising a communication from a known and trusted source to an unknown one. It can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server[48];
- *Sybil*: the attacker creates a number of fake identities through which a considerable amount of false opinions can be introduced into the system and subvert it[49].

Examples of passive attacks are the following:

- *eavesdropping*: it occurs when digital communications are intercepted with the aim of finding out confidential information, listening to digital or analogic voice communication;
- *monitoring*: the attacker can read confidential data, but it is not able to modify them[50];

[47] Paloalto networks, *What Is a Denial of Service Attack (Dos)? An Overview of Dos Attacks*. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

[48] Forcepoint, *What is Spoofing? Spoofing Defined, Explained, and Explored*. Available at: https://www.forcepoint.com/cyber-edu/spoofing.

[49] Chang Wei and Wu Jie, *A Survey of Sybil Attacks in Networks*, Department of Computer and Information Sciences Temple University, Philadelphia, 2014. Available at: https://pdfs.semanticscholar.org/97dd/43eabe4789e39b8290cf43daa513483aa4c7.pdf?_ga=2.50091172.327794438.1566547994-1479164381.1566547994.

[50] Pawar Mohandas and Anuradha J., *Network Security and Types of Attacks in Network*, Conference Paper in Procedia Computer Science, May 2015. Available at: https://www.semanticscholar.org/paper/Network-Security-and-Types-of-Attacks-in-Network-Pawar-Anuradha/2e03854bc7712720dfd6f9c2d8cb9f10082d88bd.

- *traffic analysis*: it is the process of examining network traffic to deduce information in the communication path between the sender and the receiver.

Another cyber-dependent crime in which OCGs are involved in the EU is the online child sexual exploitation (CSE), particularly for financial gain. This is a growing threat and a serious damage, facilitated by the Internet, which provides offenders an environment characterised by anonymity and safety through the Darknet. As reported by Europol[51], different forms of CSE have been detected, namely the commercial CSE, intended to satisfy the demand of mentally ill and perverted individuals with a sexual interest in children. Usually this form of CSE is associated with another significant threat, that one of Live Distant Child Abuse (LDCA). Moreover, there is a growing trend in the production of Self-Generated Indecent Material (SGIM), that consists in the sharing of indecent images of minors distributed accidentally or in malicious way without consent. Another criminal activity of CSE associated to SGIM is that one of sexual extortion, when an offender uses an explicit image of a minor to threaten and exercise coercion and extortion to the minor or alternatively seeking financial gain.[52] Child sexual exploitation is a priority crime due to the nature of the crime, the damages inflicted to the victims and the cohabitation with other forms of crimes, namely the trafficking in human beings and migrant smuggling.

4.6. Fraud schemes

Organised crime groups in the EU are involved in different types of fraud, among which: excise fraud, investment fraud, mass marketing fraud, payment order fraud and value added tax (VAT) fraud.
Excise fraud refers to the methods employed by criminals to avoid the payment of excise duties on given products (e.g. alcohol, cigarettes, mineral oils) and make profits by selling both original and counterfeit excise goods at lower prices, if compared with the market average value. Another type of fraud is that one related to investment, which employs social engineering techniques to generate profits, namely the manipulation of individuals to obtain personal and confidential information. Investment fraud is a growing threat and it is recorded to generate high profits, as demonstrated by the investigation – operation BATEO – launched in 2015 by law enforcement authorities in Germany, Portugal and Spain, which revealed the fraudulent operations of a OCG that offered investments into a music sharing platform and which was able to generate profits of more than €3 billion euros[53]. Mass marketing fraud is another form of fraud scheme employed by OCGs, which exploits social media and instant messaging applications to obtain sensitive information or payments from the victims. One example is that one provided by a UK-based OCG which generated, between 2014 and 2015, profits over €690.000 euros (£600.000 pounds) through a mass marketing fraud which had as target the

[51] EUROPOL, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
[52] Ibidem.
[53] EUROPOL, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017. Available at: https://www.europol.europa.eu/socta/2017/.

pensioners. Another fraud scheme is that one of the so-called payment order fraud or Chief Executive Officer (CEO) impersonation. This kind of fraud has as main targets organisations active internationally. The fraud schemes adopted, also in this case, rely heavily on social engineering methods and deception, to steal funds which are then transferred outside the EU. Then, the abuse of the value added tax rules for cross-border transactions generates the VAT fraud, which produces multi-billion profits by avoiding the payment of VAT. Another type of fraud is the insurance fraud, mainly targeting the health care systems. One case investigated in 2015 by German law enforcement authorities was that one of a Russian-speaking OCG providing nursing services to fraud health care insurance providers[54]. Other types of frauds are the benefit fraud, targeting labour and social benefit schemes; the EU subsidy fraud, which by means of participation in EU grants or tenders, aims to defraud the EU funds; the procurement rigging, a type of fraud linked to participation in public tenders, which consists in the use of bribes to directly influence the evaluation of bids to win a public service tender mainly in the construction, energy, information technology and waste management services and, to conclude, the loans and mortgage fraud, where the fraudsters employ false documents to obtain bank loans.

4.7. Organised property crime

Several actors are involved in organised property crime, which includes different offenders, such as organised burglaries, thefts and robberies, motor vehicle criminal groups and traffickers of cultural goods. A trend that has been registered is the increasing use of online marketplaces to sell stolen goods. As far as the extension of the phenomenon in the European Union is concerned, Europol has warned that in some countries of the EU there has been an increase in the number of burglaries reported, particularly against business sites. Furthermore, the extent and the nature of the criminal activities carried out across the EU suggest the massive involvement of mobile organised crime groups (MOCGs). MOCGs are increasingly directing their attacks against low-level commercial premises, which have at disposal far less sophisticated security measures in comparison with the security standards of banks and high-level business, against which a sharp decline in criminal actions handled by OCGs has been registered. Another interesting aspect is the use of the Internet as a facilitator. In fact, criminals obtain information about their targets employing social media platforms and fencing stolen goods in online marketplaces. Another expanding sector within organised criminal activities is the illegal online trade in cultural goods, that is expanding in the EU also due to the recent conflicts in Libya, Syria and Iraq[55]. The seize of the market is considerable and as reported by the European Commission[56] it

[54] Ibidem.
[55]UNESCO, *The Protection of Heritage and Cultural Diversity: a Humanitarian and Security Imperative in the Conflicts of the 21st century*, Background note to the International Conference "Heritage and Cultural Diversity at Risk in Iraq and Syria", Paris, December 2014 https://en.unesco.org/system/files/iraqsyriaeventbackgroundnoteeng.pdf.
[56] European Commission - Directorate-General for Education, Youth, Sport and Culture, *Illicit trade in cultural goods in Europe. Characteristics, criminal justice responses and an analysis of the applicability of technologies in the combat against the trade*, (Luxembourg: Publications Office of the European Union, 2019). Available at: https://publications.europa.eu/en/publication-detail/-/publication/d79a105a-a6aa-11e9-9d01-01aa75ed71a1.

accounts annually a total value ranging from €64 to 318 million euros. In order to contrast this illegal market at the European Union level, joint operations involving different EU Member States and Europol have been deployed. Among which the most recent are: Operations PANDORA I and II (2016 and 2017), Operation Demetra (2018) and Operation Sardica (2018). Moreover, according to the finding of the European Commission[57], evidences have been found of a link between the profits coming from illicit trafficking of cultural goods and terrorism, thus posing an alarming threat to the European Union.

Fig.7 European law enforcement operations, illicit trade in cultural goods

Operation	Lead and participating countries	Objects seized	Arrests	Investigations
Colosseum[33] [34]Nov 2011	IT, MT, EL, CY (lead); AT, BE, BG, CZ, EE, DE, HU, LU, RO, NL, SK, ES; non-EU: RU, CH, TR, UA, USA	459 objects, 32 seizures	Not known	Not known
Odysseus Jan – Jun 2014	IT, MT, EL, CY (lead); BE, BG, CZ, DE, ES, LU, HU, NL, AT, RO, SK; non-EU: RU, CH, TR, UA, USA	Not known	Not known	Not known
Pandora I[35] 17 – 23 Nov 2017	CY and ES (lead); AT, BE, BG, HR, DE, EL, IT, MT, NL, PL, PT, RO, UK; non-EU: BA, RS, CH	3.561 works of art and cultural goods; 500 archaeological objects (400 coins)	75	92
Pandora II[36] 20 – 30 Nov 2017	ES (lead for Europe); 80 other countries	More than 20.000[37] (41.000 worldwide in operation ATHENA, led by Interpol and WCO)	53*	200*
Demetra[38] 4 July 2018	IT (lead); DE, UK, ES	25.000 archaeological goods valued at 40 mEUR during action day; 3.000 archaeological goods (+ 1.000 fakes) valued at 40 mEUR.	23	1
Sardica[39] 23 Oct 2018	ES, BG (lead); also support from Eurojust	30.000 artefacts (genuine or forged); 180.000 EUR cash	13	1

Source: UNESCO, 2013; Europol, 2017; Europol 2018; UNESCO 2018.

[57] Ibidem.

4.8. Intellectual property crime

As observed by the 2019 threat assessment of Europol and the European Union Intellectual Property Office (EUIPO)[58], the counterfeit and pirated goods markets account for 6.8% of EU imports, for a total value of €121 billion euros and the trend for the following years is expected to grow. The main origin country of counterfeit goods is China, nevertheless other countries are significant for specific items. As far as the routes are considered, a new trend observed is that one of OCGs employing the new rail transportation routes opened in recent years, which connect China and the EU. A recent trend that has also been registered is related to the methods of trafficking, where there have been a significant increase in trade by means of small parcels, due to the growth experienced in the online marketplaces for illicit items. Nevertheless, most of the counterfeit trafficking to the EU takes place in freight shipping.

Furthermore, also in the case of intellectual property crime, technological advancement has had a significant impact on counterfeiting. Online marketplaces play a key role in the distribution process particularly, but also in the selling phase, as well as in the advertising through social media platforms. Moreover, the employment of technology by OCGs has determined higher revenues and demand, due also to the fact that selling on online marketplaces, and in some cases in the dark net, guarantees both a lower level of traceability and an increased level of anonymity, consequently acting as a trigger and facilitator for criminal activities. To have an idea of the extent of the counterfeiting crimes it is useful to mention Operation In Our Sites (IOS), a Europol action deployed in 2018, which resulted in the seizure of 33.654 domain names and associated online shops involved in the selling of counterfeit items for a total value of €1 million euros seized[59]. Intellectual property crimes have also consequences on the legal economy, decreasing the profits of legitimate business and depriving the governments of tax revenues. Moreover, since counterfeit items are not subordinated to any type of control and supervision, they have a considerable negative impact on the health and safety of the consumers as well, further extended by the fact that counterfeits items belong to a wide and diversified range of sectors, among which: automotive, agri-food, cosmetics, electronics, luxury, pharmaceuticals, tobacco. Considering the health threats posed by the trafficking in counterfeit goods, of particular relevance appears to be the distribution of counterfeit pharmaceuticals, as demonstrated by the investigations led by Interpol and Europol, e.g. Pangea IX in 2016, which resulted in 393 arrests worldwide and in seizure of potentially life-threatening medicines for a total value of over €50 million euros[60].

[58] EUIPO-EUROPOL, *Intellectual Property Crime Threat Assessment 2019*. Available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf.

[59] Europol, *Operation Takes Down Over 33 600 Internet Domains Selling Counterfeits Goods*, Press Release, 2018. Available at: https://www.europol.europa.eu/newsroom/news/operation-takes-down-over-33-600-internet-domains-selling-counterfeits-goods.

[60] Europol, *Online Sale of Fake Medicines and Products Targeted in Operation Pangea IX*, Press Release, 2016. Available at: https://www.europol.europa.eu/newsroom/news/online-sale-of-fake-medicines-and-products-targeted-in-operation-pangea-ix.

4.9. Environmental crime

The European Commission has defined environmental crime as "acts that breach environmental legislation and cause significant harm or risk to the environment and human health".[61]

Environmental crime generates considerable profits, it is difficult to detect and presents low sanctions, making it highly attractive for organised crime groups. Moreover, the negative impact of environmental crime involves different aspects, not only the environmental one. As a matter of fact, environmental crime affects the economy, causing losses of income to legitimate business and loss of tax revenues. It generates social damages, such as the harm caused by toxic pollution. Moreover, fighting environmental crime has costs for public administration and diverts the law enforcement authorities' resources from fighting other crimes[62]. Overall, the annual value of transnational environmental crime accounts for a value ranging from €70 to 213 billion euros annually. In Europe, OCGs are mainly involved in the illegal trafficking of waste and endangered species. Criminals involved in the illegal trafficking of waste have demonstrated a high degree of adaptability, moving in the last years towards the business model of illicit waste management and rather than just emptying waste illegally, they have generated profits from it. Considering the trafficking in endangered species, the OCGs involved present a high level of specialisation and professionalism, but their extent is limited. Nevertheless, their number is expected to growth in the following years, since the EU results to play a pivotal role in the market, being a transit region for endangered species trafficked mainly in Asia and North America.

5. The nexus between organised crime and terrorism

In recent years, the European Union (EU) has been the target of repeated terrorist attacks, whose investigation has revealed a connection between terrorism and organised crime. In particular, terrorists have used migrant smuggling networks to infiltrate their operatives in the EU. The threat emerging from the nexus between terrorism and organised crime concerns two main aspects. Firstly, the exploitation of OCG structures and networks to obtain firearms or counterfeited documents and to move people freely across the EU. The second threat-element is that one related to the financing of terrorism through the profits generated by organised crime activities[63]. According to a study conducted by the CT MORSE project, funded by the EU, there are evidences of the aforementioned nexus. The terrorists which conducted the attacks in France during 2015, for instance, were all involved in criminal activities[64]. For instance, focusing on ISIS, it has been found that 22% of the

[61] European Commission, *Combating Environmental Crime*. Available at: https://ec.europa.eu/environment/legal/crime/.
[62] European Union Action to Fight Environmental Crime, *Environmental Crime and the Eu Synthesis of the Research Project "European Union Action to Fight Environmental Crime" (Efface)*, (Berlin: Ecologic Institute gGmbH, March 2016). Available at: https://www.ecologic.eu/sites/files/publication/2016/efface_synthesis-report_final_online.pdf.
[63] EUROPOL, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
[64] CT MORSE Counter-terrorism, Monitoring, Reporting and Support Mechanism, *Examining the Nexus between Organised Crime and Terrorism and its implications for EU Programming*, 2017. Available at: https://icct.nl/publication/examining-the-nexus-between-organised-crime-and-terrorism-and-its-implications-for-eu-programming/.

terrorists which were organising attacks in the West between July 2014 and August 2014 were involved in criminal activities, mainly drug trafficking, as reported by Robin Simcox[65]. Moreover, there are evidences that the so-called foreign fighters – Europeans who have left Europe to join ISIS – have financed their activities by means of frauds and low-level criminality[66]. Moreover, a growing trend for the next years is the exploitation of the migrant flows from Middle East and Africa through the smuggling routes, which have already been employed to let enter in the EU terrorists linked to ISIS. Therefore, there is a convergence between terrorism and organised crime and, as pointed out by the study of Mullins and Wither[67], four main types of relationships have been detected. Firstly, the "interaction", where terrorists and criminals either work together or are in conflict with each other. The second type is the "appropriation", when a group incorporates the other (e.g. criminals employing terrorist tactics). A third type is represented by the "assimilation", where both terrorist and criminal activities are deployed, generating hybrid organisations. The fourth and last type of relationship analysed is the "transformation", which implies an identity shift from one category to the other.

The third type of relationship between terrorism and organised crime, that one of "assimilation", is the more likely to increase in the next years, with the emergence of always more interdependent hybrid organisations, which generate mutual benefits in terms of political and economic power to both terrorists and organised crime groups. This nexus between terrorism and organised crime can be divided in two main components, as interpreted by Makarenko[68], namely the operational component and the alliances. The former, refers to terrorists exploiting criminal activities as a source of funding, while the latter involves the building of alliances between the two groups under analysis. Nevertheless, when considering the nexus between terrorism and organised crime it is of the utmost importance to consider the theoretical and empirical findings in the specific context in which the targets operate.

6. Infiltration of organised crime groups in the European legitimate economy

As analysed by Trascrime[69], the European illicit markets generate approximately €110 billion euros each year, whose revenues are shared by a plurality of organised criminal networks and partially invested in legitimate companies to hide the illicit flows of money. In fact, evidences of laundering of illicit proceeds in the European legal economy have been detected in the European Union Member States. Furthermore, there are evidences according to which organised crime groups are gradually shifting from traditional markets (e.g. drugs and

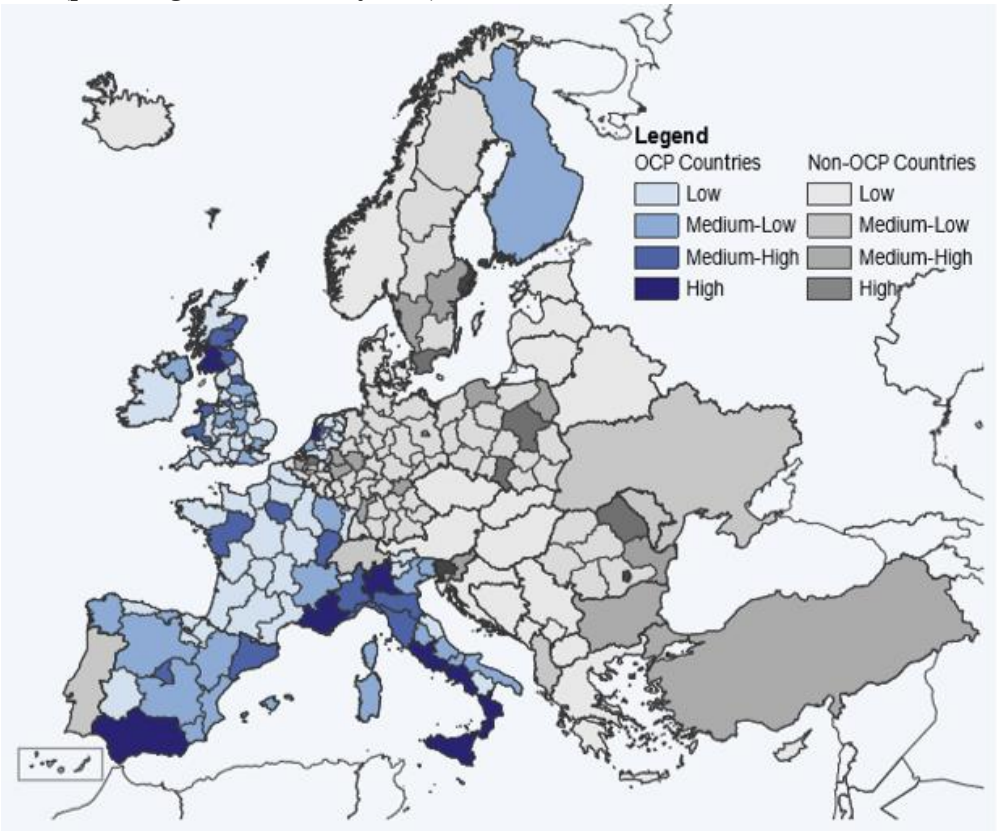
[65] Simcox Robin, *'We Will Conquer Your Rome': A Study of Islamic State Terror Plots in the West*, The Henry Jackson Society, Center for the Response to Radicalisation and Terrorism (CRT), 2015, p.3.
[66] Braw Elisabeth, *Foreign Fighters Financing*, Foreign Affairs, October 25, 2015.
Hjelmgaard Kim, *European Welfare Benefits Help Fund ISIS Fighters*, USA Today, February 23, 2017.
[67] Mullins Sam and Wither James K, *Terrorism and Organized Crime*, Connections: The Quarterly Journal, No.3, 2016. Available at: https://www.jstor.org/stable/pdf/26326452.pdf?refreqid=excelsior%3A63ce683f2047287642301f98c5aaba02.
[68] Makarenko Tamara, *The Crime–Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism*, Global Crime Vol. 6, No. 1, February 2004, pp. 129–145. Available at: https://www.iracm.com/wp-content/uploads/2013/01/makarenko-global-crime-5399.pdf.
[69] Savona Ernesto U. and Riccardi Michele (Eds.), *From illegal markets to legitimate businesses: the portfolio of organised crime in Europe*, (Trento: Transcrime – Università degli studi di Trento, 2015).

human trafficking) to less risky and highly profitable illicit activities such as fraud and organised property crime. A second observed trend is the instrumental use of covert legitimate companies in illicit markets for fraud schemes (e.g. shell companies and insurance frauds), for money laundering activities and as frontline actors of illicit trafficking (e.g. transport and shipping companies).

Considering the geographic areas where criminal investments occur, a specific concentration has been observed in Italy, particularly in the Southern regions, Lazio and North-western regions; in France, in the Provence-Alpes-Côte d'Azur, Île-de-France and Eastern regions; in Spain, especially in Andalusia, Madrid and South-eastern regions; in the UK, in London and in the South-western regions of Scotland; in the Netherlands, specifically in the areas of Amsterdam and Rotterdam; in Germany, in the Berlin-Düsseldorf-Köln area; in Romania, in the area of Bucharest and on the border with Moldova. Taking into account the assets of the organised crime investment portfolio, we can mention registered assets (e.g. cars, boat), movable goods (e.g. luxury goods, financial instruments, bank accounts), real estate properties and companies. According to the data collected by Transcrime[70], the business sectors preferred by criminal investments are bars and restaurants, casinos, slot machines, betting and gaming, construction, retail trade, transportation, real estate, tourism. Moreover, a new trend observed is the investment made by criminal organisations in the renewable energy and waste and scrap management. Considering the type and nature of the major organised groups operating in Europe, the following are the most active groups: Italian mafias, Chinese and Russian organised criminal groups. The main drivers of organised crime investments are the need to launder criminal proceeds, increase profits, obtain personal benefits, impose control over a given territory, gain social consensus through creation of job opportunities and providing public services as well as to infiltrate the local political domain. Furthermore, investments in the legitimate economy act as facilitators for the deployment of illicit activities, using for instance oil and gas companies to commit fraud or transportation and logistics companies to cover illicit goods smuggling. As far as the type of assets confiscated are concerned, it results that the overall number of confiscations increased in the last ten years and that most of the assets seized by European law enforcement authorities are movable assets, while there is a lack of confiscated companies. This last aspect represents a deficiency of the system to counter the illicit investments made by organised crime network, since there are evidences of criminal investments in a varied set of companies in Europe, whose ownership is fundamental for the overall functioning of the criminal activities carried out in Europe.

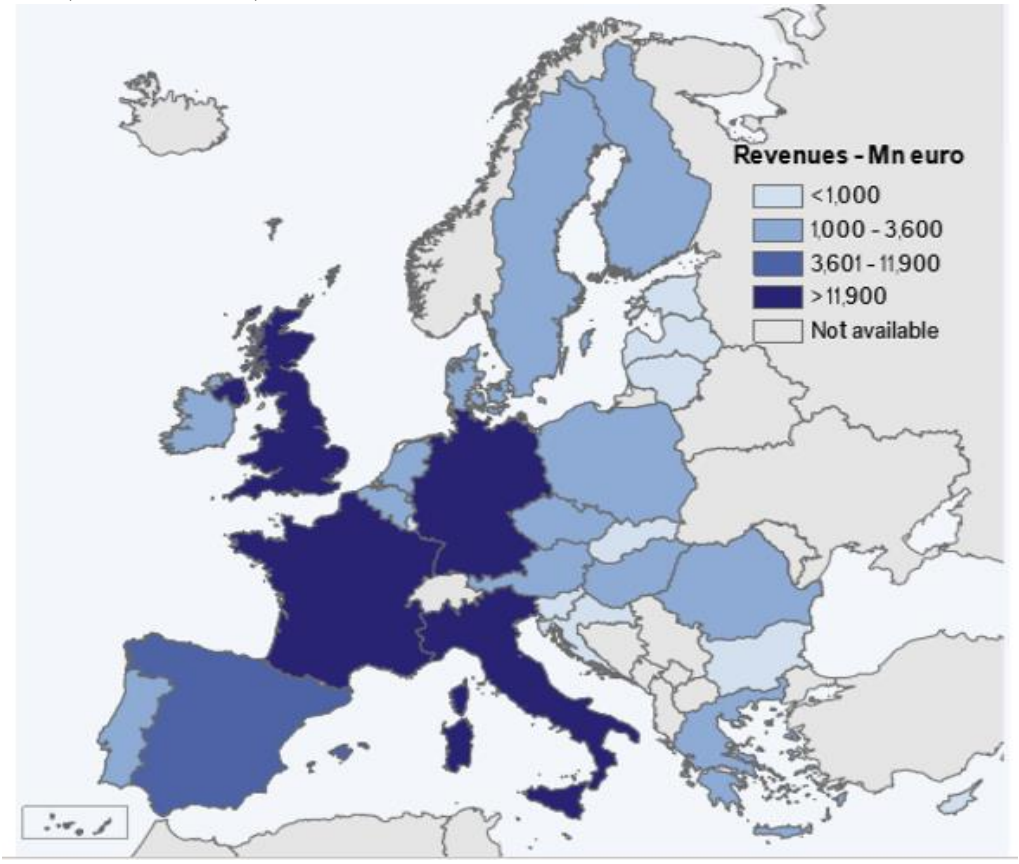
[70] Ibidem.

Fig.8 European regions with evidence of organised crime investments (percentages of the country total)



Source: Transcrime elaboration on OCP estimates, 2017.

Fig.9 Estimates of the revenues from illicit markets in the EU (absolutes values)



Source: Transcrime elaboration on OCP estimates, 2017.

II. HISTORY AND CULTURE OF RUSSIAN CRIMINALS

1. Origin and evolution

A widespread and accepted concept, at least in the Western culture, is that one of historical reconstruction, historical memory and collective memory. "Collective memory" is a concept firstly employed by Maurice Halbwachs[71] in the twentieth century, the French philosopher and sociologist systemically analysed it in connection with history and define it as the set of knowledges and representations of the history and development of a given society, which allow the individual to re-experience a particular event in the history. Collective memory stands, in a broader way, as the way an individual elaborates about its history and how perceives the history of the society of belonging. The past shapes what nations are today and how they elaborate about themselves and the others. The process of elaboration of our past, both glory and shame, allows a nation to mature and evolve, e.g. historical elaboration of Nazism and the awareness of responsibility and blame for the atrocities committed has led Germany to recreate a national and cultural identity, evolved and re-shaped by the tremendous past but aware of its fault. This process of historical elaboration and acceptance of a collective identity, which is made of both egregious and shameful events, has allowed Germany to reborn from its ashes in the aftermath of the second world war and to establish itself as a model of democracy and openness in terms of tolerance of diversities. The same did not apply to Russia, whose history has never been fully and objectively elaborated. Stalinism and Soviet ideology are still perceived by large part of the population as a period of greatness for the Russian people, notwithstanding the terror, the deportation, poverty and grievances for the lack of basic freedom rights characterising the Soviet Union[72]. The main answer to this apparently unreasonable perception among the Russians, lies exactly in the missed opportunity of an in-depth and objective analysis of the past, an element which characterises the Russian society and influences its choices, preferences and its role in the world history.

This lack of historical elaboration characterises the birth of Russian organised crime. In fact, as discussed by Galeotti, "Russian organised crime seems to reveal in its ahistoricity, lacking even a folklorish interest in its past".[73] Russian organised crime builds its identity on the present, without glorifying or blaming its past, showing a characteristic feature of the Russian contemporary society, the aforementioned, denial of historical elaboration. Nevertheless, Russia's contemporary underworld has its roots in the rise of a new generation of criminal leaders, the *avtoritety* ('authorities'), which emerged after the collapse of the Soviet Union in 1991 and consolidated their power in the transition to the market economy. The *avtoritety* shaped a new underworld, in open contraposition to the Russian criminal tradition, most notably represented by the Soviet *vorovskoj mir*

[71] Halbwachs Maurice, *On Collective Memory*, edited and translated by Lewis A. Coser, (Chicago and London: The University of Chicago Press, 1992).
[72] Svetlana Alexievitch, *Vremia second hand (konec krasnovo čeloveka)*, (Moskva, Vremia, 2013).
[73] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Heaven and London: Yale University Press, 2018), p.10.

(the 'thieves world'), which refers in turns to the *vory* subculture of the Tsarist years. What needs to be underlined is the metamorphic nature of Russian organised crime, in fact, as it will be explained in the next sections, it is clear, throughout the historical events, how the *vorovskoj mir* was able to change, adapt and even deny itself in order to survive. This is the most relevant future of *Rossijskaja Organizacija*, the struggle for survival, alongside with the connection with the State, that in the present research is called the "criminal-governmental nexus". The relevance of *Rossijskaja Organizacija* is multifaceted, it is not just an ethno-cultural fraction of the global underworld, it is not just an organised crime group, what makes it so relevant it is the capacity, specific of Russian organised crime, to influence society and the extent to which the practices, aims and paradigms of the *vorovskoj mir* have been able to delineate the boundaries of contemporary Russia.

1.1. The foundations of the Rossijskaja Organizacija

Serfdom lasted in Russia up to the 1861, when Aleksander II finally abolished it, through the *Krestjanskaja reforma* or emancipation reform, but long before that "liberal" reform, there was throughout the lands of the Russian Empire a steady movement of peasants, the so-called *krepostnoj krestjanin*, running away from their land-owning masters[74] and it is exactly in this movement of people towards freedom, since the sixteenth century, that lies the origin of the Russian criminal underworld.

The development of the first forms of Russian organised crime follow two main trajectories: rural and urban. Rural criminality, as explained by Galeotti[75], generated as a form of banditry that did not present an organised structure and developed mostly due to the absence of state policing in rural areas, where order and punishment for criminal activities was left to the so-called *samosud* ('self-judging'), a primitive and brutal but organised system of criminal justice which guaranteed the protection of villages. Among the different forms of rural banditry there is one which deserves attention due to the high degree of organisation and specialisation, the so-called *konokradami* ('horse thieves'). They presented some embryonic features which would have characterised later the *vorovskoj mir*. In fact, the horse-thieves established complex networks, including corrupted police officers, informants and other gangs in order to sell stolen horses but also the exercise a form of control over a given territory. The different status of this form of crime in comparison with the common rural banditry is also testified by the sharpness of the *samosud* applied in Russian and Siberian villages, that provided stronger and even more brutal than usual forms of punishment, due to the high-level of danger represented by the thieves of horses to the local communities[76]. Nevertheless, it is in the cities that Russian organised crime emerged and flourished during the nineteenth century, shaping the so-called *vorovskoj mir*. A number of factors have permitted the formation of a variegated criminal *milieu* in the Russian major cities

[74] Riasanovskij Nicholas V., *Storia della Russia. Dalle origini ai giorni nostri,* (Milano: Bompiani/Rizzoli Libri S.p.A., 1989/2016). pp. 369-391.
[75] Galeotti Mark, The Vory. Russia's Super Mafia, (New Heaven and London: Yale University Press, 2018).
[76] Feodorov S.G., "Obyčnoe pravo, samosud i konokradstvo v rossijskoj i sibirskoj derevnjach vo vtoroj polovine XIX veka", in *Gumanitarnye Nauki*, Vypusk 9, Vestnik Kurganskovo gosudarstvennogo universiteta, 2013.

like Moscow and St. Petersburg, among which, the most relevant are the huge wave of urbanisation during the nineteenth century and the lack of efficiency of police authorities. These two-elements combined gave birth to the *jamy* ('pits'), degraded slums at the outskirts of the urban centres, which became a prolific hub, attracting bandits and emarginated individuals in the late-Tsarists Russia, where the subculture of the *vorovskoj mir* originated. Even before the formation of the *vorovskoj mir*, characterised by a hierarchical structure, high-degree of organisation and specialisation, professionalism and cultural element (e.g. a language, *fenja*, and a symbology, represented by tattoos), there were criminal groups operating in the Russian urban ground, the so-called criminal *artel*, that imitated the general features of the original *artel*, a Russian social institution of joint labour in the agricultural, trade and construction fields. The main principles of organisation in a Russian artel, as explained by Gilinskij and Kostjukovsky[77], were: a verbal voluntary agreement, a principle of sole liability, the equality of all the members and the election of a leader (*atman*[78], "ataman" or *starosta*[79], 'elder'). What emerged as the *vorovskoj mir* was then a result of different criminal identities populating the Russian urban environment, in particular the *jamy*, characterised by different specialisations such as the *skokari* ('burglars'), the *ščipačy* and *širmačy* (pickpockets), the *maravichery* (elite pickpockets), *poezdošniki* (train-pickpockets), just to mention a few of them.

1.2. The beginning of the twentieth century: a turning point for the vorovskoj mir

The beginning of the twentieth century was marked by a sense of crisis within the Russian society, due to a number of reasons, such as the defeat in the war with Japan, the aborted 1905 revolution and the failure of Russia's engagement in the First World War. These elements, jointly with the economic and social crisis, gave birth first to the bourgeois Revolution of February 1917, followed by the proletarian October Revolution of the same year and subsequently to the Civil War of 1918-22. What results of interest for the present research is to analyse the effects of these major events on the Russian criminal underworld. In March 1917, a general amnesty was granted by the Provisional Government and thousands of criminals were released. Moreover, the different criminal groups operating throughout Russia participated in the civil war, acting on behalf of the counter-revolutionary army (*Beloe dviženie*, the 'white movement'), the revolutionary armies (*Rapoče-krest'janskaja armija,* the 'Workers' and Peasants' Red Army') or the independent forces (*Zelënaja Armija*,

[77] Gilinskiy Yakov and Kostjukovsky, "From Thievish *Artel* to Criminal Corporation: The History of Organised Crime in Russia" in Fijnaut Cyrille and Paoli Letizia, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004).

[78] The Russian word *атман* ('*atman'*) referred originally to a military title, employed in the Russian Empire, owned by the leaders of the Cossack armies. The title was then abolished under Catherine II in 1764. In the context of the Russian criminal underworld it was used to indicate the leader of a group.

[79] The word *староста* ('starosta') referred, in Slavic countries, to the figure of the elder in a clan, responsible for the management of the community's assets. This term has been employed throughout the history both in Russian and other Slavic country as a synonym of leader. It has yet a contemporary usage in Russia, e.g. within the university, the *starosta,* is the student-group leader.

the 'Green Army'), depending on the convenience. In addition, as reported by Gilinskiy and Kostjukovsky[80], due to the political turmoil and power *vacuum* the actions of Russian criminal gangs intensified considerably during the civil war years, terrorizing all the major Russian cities. Several criminal groups were active in Petrograd under different gangsters, such as Lën'ka Panteleev, Miška Panyč, Ivan Zatotsky (gang of Vanka Kukolka), Ivan Belov (gang of Vanka Belka). Moscow as well had a diversified criminal environment of gangs, among which that one of Nikolaj Safonov (Saban gang) or that one belonging to Saška-Seminarist. Such a wide spread of criminal activities required a strong action on the part of the authorities, which also resort to the army to maintain order. However, at the end of the Civil War in 1920, the situation in the country appeared to be stabilised and by the end of 1927 the criminal gangs operating throughout the country were almost dismantled and the criminal underworld was subjected to a significant internal transformation. In the aftermath of the Civil War, an increased number of criminals were jailed or sent to the labour camps. As reported by Gilinskiy and Kostjukovsky[81], a quarter of the prison population was constituted by professional thieves and among them authority figures called *urka* or *urkagan,* belonging to the traditional "old" underworld, and "new" criminals characterised by a more ideological behaviour of opposition to the Soviet authority, which were called *jigan*. From the war between these two different criminal forms, *urka* and *jigan,* which ended with the victory of the first, a new form of criminal underworld was born, closer to contemporary *Rossijskaja Organizacija*, that one of the *vory v zakone* ('thieves-in-law').

1.3. The thieves-in-law

The thieves-in-law represented moral authorities within the *vorovskoj mir*, professional criminals obeying to an unwritten code or rules of behaviour, whose infringement predicted serious punishments. This new form of organisation of the criminal underworld, emerged as a result of the troubled Civil War years, was forged and paradoxically unified by the Gulag system of labour camps, engineered by Joseph Stalin during the 1920s. The General Directorate of Forced Labor Camps, commonly known as Gulag (in Russian: *Glavnoe Upravlenie ispravitel'no-trudovych Lagerej – GULag*) were established under Lenin but were systematically exploited for deportation of general criminals as well as political opponents under Stailn. As it is stated by Graziosi, the Gulag were an attempt to economically reorganise the penal system and to tackle the economic deadlock, without placing burdens on the State budget[82]. The number of prisoners within the Gulag system has been analysed by Applebaum, that estimates a total number of 29.7 million of prisoners from 1929 and 1953[83]. Therefore, the Gulag system constituted a real double world, which included most of the criminal underworld

[80] Gilinskiy Yakov and Kostjukovsky, "From Thievish *Artel* to Criminal Corporation: The History of Organised Crime in Russia" in Fijnaut Cyrille and Paoli Letizia, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004), pp. 189-191.
[81] Ibidem.
[82] Graziosi Andrea, *L'URSS di Lenin e Stalin. Storia dell'Unione Sovietica 1914-1945*, (Bologna: Il Mulino, 2007), pp. 255-294.
[83] Applebaum Anne, *GULAG. A History*, (Great Britain: The Penguin Press, 2003).

of those years. Nevertheless, instead of eradicating the problem of criminal groups in Russia, the Gulag became the playground of the thieves-in-law, which became more homogeneous and extended their network including also non-Slavic nationalities and imposing themselves as the leading figure within the Russian criminal underworld.

Given the role acquired, the thieves-in-law underwent a process of "institutionalisation" of their structure and rules, with the establishment of a Code. Finckenauearn and Waring in their research have listed a set of principles of the Thieves Criminal Code, among which, the most relevant are the following:

- The *vor* must live only by criminal activity and it is forbidden to work;
- The *vor* must not have a family except for the criminal community that is his family;
- The *vor* must provide moral and material assistance to his criminal community;
- The *vor* must not become involved with the authorities or any social organisation;
- The *vor* must not serve in the military;
- The *vor* must obey to and carry out the punishment provided by the thieves' meeting (*šodka*).[84]

Moreover, as referred by Gilinskiy and Kostjukovsky[85], the thieves-in-law established a tight hierarchy, with different castes, defined *mast* ('suit') in *fenja*, the criminal language. The highest caste was that one of the *vory v zakone* ('thieves-in-law'), while subordinated castes were represented by the *mužik* ('peasants') and the *frajer*[86] ('free person', common citizens). There were also dishonourable castes, such as the *pidor* (very offensive word to indicate homosexuals), the *krysa* ('rat', it indicates individuals stealing from the criminal community), the *stukač* ('informer') and the *čušok* ('wretch', a despicable or contemptible person). The Thieves-in-Law Code established also a set of "institutions", among which it is worth mentioning two of them. The *šodka*, a general meeting of all the thieves-in-law where, among other things, the punishments for the transgressors of the Code were decided and the *obščak* ('common fund'), to which all the members of the criminal community had to pay a contribution.

[84] Finckenauer James O. and Waring Elin J, *Russian Mafia in America: Immigration, Culture, and Crime,* (Boston: Northeastern University Press, 1998).

[85] Gilinskiy Yakov and Kostjukovsky, "From Thievish *Artel* to Criminal Corporation: The History of Organised Crime in Russia" in Fijnaut Cyrille and Paoli Letizia, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004), pp. 193-195.

[86] The Russian word *фрáĭер (frájer*) is a borrow from Yiddish פֿרייַער (*frayer*, 'free person'), from פֿריַי (*fray*, 'free'), which in turn borrowed the term from the German *Freier* ('customer of prostitutes'). It is relevant to illustrate the etymology of the term in order to understand the development of the Russian criminal language. The term originally was used by prostitutes in Odessa's criminal underworld to refer to the clients. It was used by the Thieves-in-Law Code to indicate someone who has never been in prison. Thus, the literally meaning of *frajer* ('free person') had not a positive sense, rather a pejorative, negative one. For more information see: Zornickij A.V., *Evrejskie Ètimologii Russkich Ugolovnych Argotizmov i Metodologičeskie Trudnosti ich Izučenija*, UDK: 811. 411. 16: 81-13. Available in Russian at: http://eprints.zu.edu.ua/9183/1/12zaveer.pdf.

1.4. The 'suč'ja vojna'

A major change was then brought by the Great Patriotic War (*Velikaja Otčestvennaja Vojna* in Russian) against Nazi Germany, during which was decided to employ the convicts as soldiers, giving them freedom in exchange of serving for the military. The decision of the Soviet government, triggered by the wartime difficulties, generated a division within the criminal underworld, namely between those that left the Gulag to fight in the army, and those criminals that remained faithful to the thieves-in-law Code and refused to join the army. In the aftermath of the second world war, the former convicts, which had joined the army and survived, returned from the front. Few of them became officers, while the majority came back to their former criminal activities. As a result, part of this second group ended up in the prison camps and it is exactly in the Gulag where began the open confrontation between the thieves-in-law which did not break the Code during the wartime and refused to join the army on the one hand, and on the other, those which did it, the so-called *suki* ('bitches'), as a sign of contempt. Therefore, from 1948 until Stalin's death in 1953, the situation in the Gulag was characterised by a real war, the so-called *suč'ja vojna* ('bitches war'). The administration of the Gulag did not interfere openly in the confrontation, taking advantage of the massacres going on in the labour camps, which would have decimated the criminal community, regardless of the part who would have won. Nevertheless, the administration of the penitentiaries favoured the *suki*, among which there were also a number of informants, at the expense of the thieves-in-law. As a result, the *suki* won the fight against the thieves-in-law and when massive releases took place, due to the post-Stalin amnesty of 1953, the former convicts poured again into the cities and gave birth to a new generation of criminals. The *vorovskoj mir* was reshaped in their own image but retaining most of the thieves-in-law Code and amending some parts, most notably, that one about the prohibition to cooperate with the State. In fact, it became permissible to collaborate with the State, if it was compliant with criminal's interests. This apparently not so relevant change in the Code of the *vorovskoj mir*, had a major impact on the development of criminality in Russia and on the establishment of a "criminal-governmental nexus" that still in the twentieth century characterised organised crime in Russia.

1.5. The weakening of the vorovskoj mir and the rising of the avoritety

The years in the aftermath of Stalin's death were characterised by the leadership of Chruščëv and the so-called "thaw", a denouncement of Stalin's atrocities and a process of reformation of the Soviet Union. As far as the criminal underworld under Chruščëv's leadership is concerned, the main trend was that one of the eradication of criminal gangs. This aim was achieved through strong means of repression such as the *milicija* (police), the political police known as the Committee of State Security (*Komitet gosudarstvennoj bezopasnosti – KGB*) and the 1956 Law on Measures For Improving the Performance of the Soviet Union Ministry of Internal Affairs[87].

[87] Galeotti Mark, The Vory. Russia's Super Mafia, (New Heaven and London: Yale University Press, 2018), p.86-87.

As a result, the *vorovskoj mir* began to die as a form of subculture separated from the rest of the society and their number was drastically reduced. If the *vorovskoj mir* was fragmented and weakened by the governmental action, on the other side a rise in criminal gangs was registered. Sometimes, these street gangs evolved into organised crime and, what is most relevant is that they began to establish a perverse relation with the institutional framework, exploiting the opportunities offered by the black-market. Particularly, they provided protection for the entrepreneurs operating in the black-market, the so-called *cechoviki* or *tenevniki* ('shadow men') and by guaranteeing the movement of illegal goods in cooperation with the *farcovščiki*[88], which were then smuggled within the Soviet Union, and by paying bribes to corrupted officials. As analysed by Galeotti, a trinity emerged, constituted by corrupt officials, gangsters and black marketeers, which was increasingly institutionalised under General Secretary Brežnev (1964-82)[89] and whose infiltration in the economic and political tissues of Soviet Union became endemic under the last General Secretary of the Communist Party of the Soviet Union, Michail Gorbačëv. In 1985 Gorbačëv took the position of General Secretary and began a process of economic, political and social reform of the Soviet Union, famously known as *perestroika* ('restructuring'), completed by the *glasnost* (improperly translated as 'openness, transparency', while literally means 'advertising' as noticed by Riasanovsky[90]). This process led to a limited liberalisation of the economy and the creation of particular forms of private business (the so-called 'cooperatives'), which jointly with the anti-alcohol campaign opened a window of opportunities to the criminal groups. It was exactly under Gorbačëv that the gangsters emerged in the aftermath of Stalin's death and turned to businessmen, as a result of the strict cooperation of the criminal underworld with the upperworld of the Russian society, namely the political and business élite. Among this new class of suit and tie criminals another group emerged as the so-called "professionals of coercion", as defined by Galeotti. This last category, which remained strictly tight to the original violence of the criminal underworld, was composed mainly by sportsmen, unofficial bodybuilders (*kački*) and the veterans of the war in Afghanistan (1979-88), the so-called *afgancy.*

By the end of the 1991, at the time when the Soviet Union was collapsing, organised crime was a pervasive force in the society, having infiltrated all the societal sectors from the economic to the political level. The transitional phases in history, as explained by Di Nolfo, bring to a system of deep uncertainty, of fluidity as well as innovation, where the actors involved are not clearly defined[91]. It is exactly in the ability to exploit the vulnerabilities of the new system where lies the main reason of the rise of the *avoritiety* within the Russian Federation. Under El'cin's presidency, characterised by the economic crisis and the attempt of state building and transition to a market economy, organised crime flourished and had the chance to climb the social ladder taking advantage of the legal, cultural and social crisis, as well as of the huge privatisation campaign enhanced

[88] The Russian slang word *фарцовщики* (*farcovščiki)* indicate a category of people purchasing consumer goods and currency from foreigners in order to smuggled them within Soviet Union. The name of this illegal business activity was *фарцовка* (*farcovka*).
[89] Galeotti Mark, The Vory. Russia's Super Mafia, (New Heaven and London: Yale University Press, 2018), p. 89.
[90] Riasanovsky Nicholas V., *Storia della Russia. Dalle Origini ai Giorni Nostri*, edited by Sergio Romano, (Milano: Bompiani, 1989/2016).
[91] Di Nolfo Ennio, *Storia delle relazioni internazionali. Dalla fine della guerra fredda ad oggi*, (Bari: Laterza, 2016).

in these years. As the State was fading away, organised crime was imposing its power, establishing itself as an alternative to the State and satisfying the people demand of basic needs and offering protection, the so-called *kryša* ('roof') in the criminal slang. The supply of protection is the main feature which nearer Russian organised crime to the 'mafia' as outlined by Varese[92]. However, a further change in the balance of power between the State and organised crime in Russia was determined by the advent of Vladimir Putin to power and the reestablishment of a strong and pervasive state, which subjugated the criminal underworld, which nowadays is present but not on an equal foot, rather at the service of the State. At the beginning of the 21th century, the old tradition of the *vory v zakone* preserved just a symbolic and mythological stance, losing all its strength and original meaning. Some of the institutions and figures of the old system were maintained but deprived of their significance by the emergence and consolidation of power of the new criminal caste, the *avtoritety*, criminal-businessmen, whose activities' portfolio ranges from legitimate and illegitimate sectors of the economic and political domains.

2. Russian criminal culture

2.1. The criminal language: ofenskij jazyk/fenja

Wilhelm von Humboldt wisely asserted that a language is the phenomenal manifestation of the spirit of the people[93]. According to the Prussian scholar, to understand a nation it is essential to know its language, because the language shows how the people elaborate about themselves and the "other", how a people perceive the reality. Knowledge of the language of a given population, allow us to understand how their minds work, what triggers their actions, what is most valuable in a culture. In the present research a brief *excursus* on a specific category of the Russian language will be provided, that one of the criminal language, the so-called *ofenskij jazyk* or *fenja*. The study of *fenja*, whose origin traces back to Middle Ages, is relevant from different perspectives, as the contribution given to the creation of the criminal culture, the strengthening of the solidarity among the criminals, the belonging to the same 'family' as well as providing a feeling of identification within a group separated from the common society and allowing to communicate without being understood from those outside the community of belonging. What is most interesting is the fact the *fenja*, even if radically transformed throughout the centuries, is still spoken within the criminal communities and it is still perceived to be a threat, as demonstrated by a law emanated in the Russian Federation on 2013 prohibiting the use of the *fenja* in prisons[94]. There is no consensus regarding the origin and etymology of *fenja* and different hypotheses have been put forward. Originally, *ofenskij jazyk*, denotated the language employed by the *ofeni* ('wandering merchants') in the Middle Ages, which created a new linguistic system over the existing Russian to

[92] Varese Federico, *The Russian Mafia. Private Protection in a New Market Economy*, (Oxford: Oxford University Press, 2005).
[93] Von Humboldt Wilhelm, "Latium und Hellas oder Betrachtungen über das classische Alterthum", in *Ausgewählte Schriften (*Berlin: Zenodot Verlagsgesellschaft mbH, 2014).
[94] Gazeta.ru, *Minjust zapretil arestantam materit'cja i «botat' po fene»*, 14th Janyary, 2016. Available at: https://www.gazeta.ru/social/news/2016/01/14/n_8117915.shtml.

communicate "*ne dlja čužich ušej*" ('not for the ears of others')[95]. Therefore, it emerged as a parallel linguistic register, to protect communication. Then, the language of the *ofeni* was assimilated by the *ugolovnyj žargon*, the modern criminal jargon (also known as: *vorovskoj žargon* and *blatnoj žargon*), at the beginning of the twentieth century. As analysed by Gračev[96], it is exactly in the Gulag system that the *ofenskij jazyk* was incorporated within the criminal jargon and was renamed *fenja,* to indicate the criminal jargon, distinguishing it from the *ofenskij jazyk/ofenja*. *Fenja* became then the language of the thieves-in-law and generally of the criminal underworld, whose members were able to '*botat' po fene'*, which can be translated from *fenja* to English as 'to speak the criminal jargon'. Analysing the aforementioned jargon expression, it is clear the difference with the Russian language, where the verb 'to speak' is *govorit*' and not *botat'*, a term whose etymology is probably Russian, from the word *boltat'*, which means 'to chat/talk a lot'. This is just an example of many that could be done to underline the interdependence of the two linguistic systems – Russian language and *fenja* – as well as their mutual extraneity. Within the criminal world, to have a good command in *fenja* was considered a sign of prestige and distinction, indicating that an individual was part of the *byvalye arestanty* ('expert prisoners'), as explained by Zugumov[97], with respect for the thieves-in-law rules and culture. For this reason, there are a number of expressions in *fenja* with an ironic and disdain meaning to indicate those people who did not speak *fenja* or pretended to know it or even those individuals, which were able to understand that language without being a criminal, as indicated by the expression *fenja v botach* which means ' to know the criminal jargon without being part of the criminal underworld'. Moreover, the language is never neutral and it is both a sociological and psychological phenomenon, that provides to the observer valuable information about the speaker, his or her sociocultural extraction, geographic origin, believes, attitudes and mentality. Therefore, paying attention to the *fenja* and the criminal jargon in general, means to acquire a deeper and more comprehensive knowledge of the Russian criminal phenomenon. The criminal language can be defined a closed system, since its main function is secrecy[98], thus can also be defined a *tajnyj jazyk* or *potajnoj jazyk* ('secret language'). As pointed out by the research conducted by Lichačev, there are a number of arguments to support the thesis of *fenja* being a secret language, among which, for instance, the fact that it has a limited vocabulary or expressions covering just a limited range of phenomena, but over all the main characteristic of *fenja*, namely the "unintelligibility for the uninitiated"[99]. Nevertheless, as observed by Timroth[100], the Russian argot[101] does not aim at conspiracy and cannot be described as artificial. Always Timroth has suggested to understand *fenja* as one way through which emarginated groups within the society communicate among

[95] Gračev M.A., *Blatnaja Muzyka*, Journal «Musart» №3, vesna 2006.
[96] Gračev M.A, Mokienko V.M., *Russkij žargon. Istoriko-étimologičeskij slovar'*, (Moskva: AST-Press, 2009).
[97] Zugumov Z.M., *Russkojazyčnyj žargon. Istoriko-étimologičeskij tolkovyj slovar' prestupnovo mira*, (Moskava: Knižnym mir, 2015).
[98] Michaeljan M.E., *Some Pragmalinguistic Peculiarities of Criminal and Pseudo-Criminal Types of Discourse*, (Pjatigorsk: Pjatigorskij Gosudarstvennyj Lingvističeskij Universitet, 2017).
[99] Lichačev D.S., "Argotičeskie slova professional'noj reči" in *Razvitie grammatiki i leksiki sovremmenogo russkogo jazyka*, Moskva, 1964. pp. 311-359.
[100] Timroth V.W., *Russian and Soviet Sociolinguistics and Taboo Varieties of the Russian Language (Argot, Jargon, Slang and "Mat")*, (München, Verlag Otto Sagner, 1986). p. 79.
[101] The *argot* is defined by the Oxford Dictionaries as "the jargon or slang of a particular group or class".

themselves[102]. Later, *fenja* would have also influenced Russian culture and language and even if common Russian-speakers may have some knowledge of the criminal language, it is perceived to be a crypto-language in continuous evolution and fully comprehensible only by those employing it constantly and it remains a "negative act of identity" whose aim is to deliberately exclude the outsiders[103].

Moreover, it has been observed how Russian argot was employed not only by specific groups of the society, such as prisoners or thieves, but also by the law enforcement authorities, like the KGB. Members of the KGB have coined for instance a number of names which entered in the usage of *fenja*, such a*s bomž* or *bomžik* ('without a fixed residence') or *boz* ('without a regular work')[104]. Camp administrators in the Soviet Union as well have invented some words of the *fenja*, such as *domušniki* ('burglars'), *medvežatniki* ('robbers') or *sutodača* ('daily ration')[105]. This second example is particularly meaningful since it highlights another important aspect of *fenja*, namely the mixture with the prison jargon. As observed by Olenik[106], to understand the contemporary *Rossijskaja Organizacja*, both in Russia and outside, it is necessary to analyse the prison culture, in fact, the experience of the Stalinist labour camps in the 1930s played a pivotal role in the formation of the criminal community. Nevertheless, *fenja* it is not limited to the influence of the prison jargon, but it presents borrowings of different languages in specific domains, such as: English loans, which appeared in the late 1960s and are still employed by speculators and currency black-marketeers. Examples are the words *baksy* and *griny* ('dollars', respectively from the American slang words 'bucks' and 'green'); then German words, which are not more used, like the word *bundes* ('West German citizens'); Italian loans like the word *putana* ('prostitute'); Swedish slang words spoken in Finland like *fjurka* ('Western foreign currency') and borrowings from Yiddish, like *drek* ('shit', 'rubbish') a word used to express an evaluation of people or objects[107]. From the analysis of Zornickij[108], it emerges that borrowings from Hebrew and Yiddish are particular prolific, due to the historically large Jews population in the Russian Federation[109] and the influence exercised by Jewish culture on the country. Other examples of words employed by the criminal jargon with origin from Hebrew or Yiddish are, for instance, *šmon* ('personal search', 'search in the barrack'[110]), *urka/urkagan* ('person convicted

[102] Timroth V.W., *Russian and Soviet Sociolinguistics and Taboo Varieties of the Russian Language (Argot, Jargon, Slang and "Mat")*, (München, Verlag Otto Sagner, 1986), pp. 88-89.
[103] Koskensalo A., *Secret Language Use of Criminals: Their Implications to Legislative Institutions, Police, and Social Policies*, Sino-US English Teaching, Vol.12, No. 7, July 2015.
[104] Ibidem.
[105] Ibidem.
[106] Olenik A., *Un double monstrueux: la culture criminelle en Russie post-sovietique*, Cultures & Conflicts 42, June 2001.
[107] Timroth V.W., *Russian and Soviet Sociolinguistics and Taboo Varieties of the Russian Language (Argot, Jargon, Slang and "Mat")*, (München, Verlag Otto Sagner, 1986). pp. 107-110.
[108] Zornickij A.V*., Evrejskie étimologii russkich ygolovnych argotizmov i metodologičeskie trudnosti ich izučenija*, Novitnja filologija (41), 2012, pp. 63-79.
[109] Drastically reduced from the late 1990s to the beginning of the XXI century, shrinking from 1.479.732 in 1989 according to the Soviet Census to 460.000 in 2000 (The YIVO Encyclopedia of Jews in Eastern Europe) and dropping down to 172. 500 according to the estimates of Hebrew University demographer Sergio DellaPergola. Nevertheless the huge contraction of Jews in the Russian Federation during the last decades, Russia is still among the countries with the largest Jewish community.
[110] Zugumov Z.M., *Russkojazyčnyj žargon. Istoriko-étimologičeskij tolkovyj slovar' prestupnovo mira*, (Moskava: Knižnym mir, 2015).

of felony'[111]), *stukač/musor* (literally 'garbage' and employed to indicate an informant[112]). Moreover, as explained by Krylosova, a new wave of vulgarisation of the language occurred at the beginning of the twentieth century, a process of mutual exchange between the different jargons (among which the criminal one) and the Russian standard language, which led to a revival of criminal jargon words in the daily communication and to an expansion in the vocabulary of the criminal jargon due to the borrowings from the official language[113]. As far as the language of the contemporary Russian criminal underworld is concerned, a set of examples can be provided to show the relevance that the criminal jargon still has nowadays. An interesting research about the nicknames of the person in the contemporary criminal world is provided by Gološčapova and Mirmovič[114], which emphasised the use of symbology within the criminal community, particularly related to the names, as a sign of distinction from common society and as a mark of identification and belonging to the criminal underworld, as well as an identifier mechanism for the criminal attitudes and characteristic of a given individual. For instance, the word *myš'* (litteraly 'mouse') indicates a pocket thief operating in the underground; *syroežka* refers to a food thief; a *tonkaja provoloka* is an agile thief; *šimbala* defines a low-level thief; *čistaja duša* (litteraly 'pure soul') indicates a thief respecting the criminal custom and rules; the word *mazicha* refers to an experienced thief. As regards the last example, that one of the 'experienced thief', there is a plethora of synonyms to define it, among which: *avtoritet, bojarin, bugor, kozyrnyj, pachan*[115]. Moreover, the aforementioned research of Gološčapova and Mirmovič, has underlined also the differences in the criminal jargon to indicate the adult and the young thieves. For instance, young or unexperienced criminals are called in the criminal jargon: *gol'čik* (meaning in English: 'beginner, wreck'; correspondent words in Russian: '*ostov, načalo'*), *kotjur* (meaning in English: 'teenage thief'; correspondent to the Russian central dialect words: *mal'čik, paren'*) *komsa* (meaning in English: 'piece, chunk'; correspondent to the Russian verb *krošit,* 'to crumble'); *mukrucha* (meaning in English: 'teenager linked with the criminals', from the Greek word *mikros, '*small'). There are also a number of words indicating women operating in the criminal underworld such as: the general name *mamoj* ('mom'); *bitoj* to indicate a high-level woman criminal; *mazyka* for a woman with experience in the criminal underworld and *nadëžnaja* for a new-entry[116]. There are also several words to indicate the women, among which personal names like *Marta* or *Maška*, and words such as *ryba* (literally 'fish'), *čuvyrla* (no literal meaning in Russian)*, čubačka* (literally 'little guy'), *koška* (Russian diminutive of 'cat'), *koška blatnaja* (meaning in English: 'thief's woman accomplice or woman robber'; no literal meaning in Russian) *mentovka kumovaja* (meaning in English: 'woman informant'; no literal meaning in Russian)[117]. There is also a set of words to denominate the criminal, such as: *žul'ban* (compound of the two Russian words:

[111] Ibidem.
[112] Ibidem.
[113] Krylosova S., *Les particularités d'emploi des mots argotiques en russe contemporain*, Cahiers du DNPS : Linguistique et politique, 2003.
[114] Gološčapova T.G., Mirmovič T.D., *Naimenovanija Lica v Kriminal'nom Mire*, Vikitimologija 1(7), 2016. pp.18-23.
[115] Ibidem.
[116] Ibidem.
[117] Ibidem.

žul', from the Moscow dialect, with the meaning of 'thief, fraudster' and *ban*, 'mob, gang'); *Jurik* (from the verb of the criminal jargon *iurit'* which means in English 'rush around'); *šajka* that refers to a group of people with criminal objectives. Terms to indicate the different roles within the criminal world are the following: *bratan* ('brother') is a member of a criminal group; *kryša* ('the protector') to indicate criminals which exercised control over given commercial activities, forcing them to pay protection money; *blatnoj* indicates someone who has close contacts with a superior; *šestërka* is a low-level criminal; *pacan* is a young criminal.

There is also a vocabulary in *fenja* indicating different professions/specialisations in the criminal underworld such as: *banovoj špan, majdannik, majdanščik*, terms referring to a criminal operating in the train stations or the underground; *gastrolër* and *zalëtnyj* referring to a thief acting outside the city; *šnifer domašnij*, a local thief; *morošnik* and *christoslavec*, thieves robbing from churches; *juvelir*, a thief stealing only gold[118]. Gološčapova and Mirmovič in their research analyse also the vocabulary in the criminal jargon to indicate other ethnicities, since the Russian contemporary criminal world is increasingly constituted by people with different ethnic origins. For instance, each non-Russian is called *mungus;* an individual from Kazakhstan is a *nosorog; černyj bolt* is a pejorative term to indicate a black person; Jews are referred to with words like *cerusalimec, tartar, udablennyk, obrezannyj*; a man of Tatar nationality is *jurok*, while a woman of the same nationality is a *širokopolaja*.

Moreover, there are terms used within the Russian organised crime to indicate different hierarchical roles, which are drawn from the criminal jargon of the drug market, such as: *baryga* ('drug dealer') which it is employed in the meaning of 'reseller of stolen goods'; *bojarin* ('drug sales organiser') used to indicate 'leader of a criminal group'; *d'javol čërt* ('first-time drug') in the sense of 'criminal wanted'; *edinoličnik* ('hemp grower' used with the meaning of 'lone thief')[119].

There is also a variegated vocabulary, connotated by a pejorative character, to indicate law enforcement authorities, such as the words: *musor* ('garbage') from the Hebrew mùser, 'guide'; *ment*, from the Hungarian name for the jacket of the Austro-Hungarian army's uniform (*mente* in Hungarian and *mentik* in Russian), a term employed in the Gulags to indicate the jailor; the word *gat*, to indicate a law enforcement authorities, from the Russian words *katorga* ('life imprisonment') or *kat* ('executioner'). Often, words related to the animal world are employed to refer to the authorities such as: *sobaka* ('dog'); *legavye* ('pointing dogs'); *barbos* ('watchdog'); *pës* ('mutt'); *suka* ('cunt'); *djatel* ('woodpecker'); *zmej* ('snake'). Specifically, Italian police corps are indicated according to the uniforms' colour as follows: *sinie* ('the blues') for the police; *čërnye* ('the blacks') for the 'carabinieri'; *serye* ('the grays') or *mestnye* ('the locals') for the local police. While the police stations are named: *musarnja*, *gadilovka* and *mentovka*.

There are also a number of expressions signalling the danger to be caught like: *atanda* used with the meaning of 'danger'; *stojat'na atande* employed to indicate 'pay attention and alert the accomplices in case of danger'; *atasnik* is someone in danger while committing a crime; *vasser* a term employed as warning with the meaning

[118] Ibidem.
[119] Ibidem.

of ‘attention’ in the Odessa dialect and used in the criminal jargon in the sense of ‘failure’, the same meaning expressed by *golvyjvassor; voda,* litteraly ‘water’, is used as a warning signal; *byt’/stojat’na strëme* (‘be the lookout’); *vasja* a warning signal with also the meaning of ‘policeman’; the term *zeks,* ‘alarm’. As far as the criminal actions are concerned, *dvižucha* indicates a theft; while a *mokroe delo* (‘wet deal’) is a homicide and a *suchoe delo* (‘dry deal’) is a criminal action without killings[120].

As last examples is useful to consider the use of the criminal jargon in relation to the drug market, since Russia organised crime is particular active in that domain.

As pointed out by Corbelli[121] each product of the drug market has its set of names in the criminal jargon. As far as the heroin (in Russian *geroin*), it is called in different ways, such as: *Gerasim*, German or *Griša*, male proper nouns; *èjč*, letter «H» pronounced in English and written in Russian; *Gerbalajf*, proper noun of a firm; *perec* (‘pepper’); *chmuryj* (‘gloomy’); *tëmnyj* (‘dark’); *gavno* (‘shit’). Considering cocaine (in Russian *kokain*), the terms employed are: *Nikolaj Nikolaevič* (proper noun and patronymic), *ganža, kokos* (‘coconut’), *koks* (‘coke’), *sneg* (‘snow’), *mel* (‘chalk’), *nomer odin* (‘number one’) and *pervyj* (‘first’). The methadone (in Russian *metadon*) is called in the criminal jargon: *lošadka* (‘filly’) and *voda* (‘water’). Terms indicating the amphetamine (in Russian *amfetamin*) are: *Fedja* (Russian diminutive of the male personal noun *Fëdor*), *amfa* (abbreviation of *amfetamin*), *vitamin* (‘vitamin’), *spidy* (from the English ‘speed’), *skorost’* (‘speed’), *šustryj* (‘fast’), *bystryj* (‘rapid’), *kapča* (English acronym ‘captcha: completely automated public turing test to tell computers and humans apart’). Lysergic acid diethylamide (LSD), also known as acid, is referred to with the following terms: *Liza* (diminutive of the Russian personal name *Elizaveta*), *Ljusja* (diminutive of the Russian personal name *Ljudmila*), *microdot* (English word indicating a tiny tablet containing LSD), *dvadcat’ pjatoe* (twenty-five), *lizer* (from ‘lysergic acid’), *kislota* (‘acid’), *limon* (‘lemon’). Another drug, ecstasy (in Russian *èkstasi*) is called: *vitamin E* or just *E* or *Éška* (term of endearment for the letter «E»), *rejv* (‘rave’). The vocabulary employed to define the marijuana (in Russian *marichuana*) are: *Marija Ivanova* (Russian female personal name and patronymic), *Mara* and *Maša* (diminutives of Russian female personal name *Marija*), *Mèri* (from the English Mary), *anaša*, *baš* (from the English ‘bash’), *belladonna* (from the name of a poisonous plant), *ded* (‘grandfather’), *djadja* (‘uncle’), *šiški* (‘pieces’). The hashish (in Russian *gašiš*) is defined by the words: *Galja* (diminutive of the Russian female personal name *Galina*), *Gennadij* (Russian male personal name), gaš or gèš (abbreviation of the Russian word *gašiš*), *dur’* (‘ passing fancy’), *garson* (form the French *garçon,* ‘young man’), *kamen’* (‘stone’), *chleb* (‘bread’)[122]. Moreover, any drugs in the form of pills is called *koleso*, meaning in Russian standard ‘wheel’, while a diluted or ruined drug is defined *golvj vasser*[123].

[120] Corbelli M., *Traducibilità del gergo criminale russo nelle intercettazioni telefoniche in Italia,* (Milano: Fondazione Milano, 2013).
[121] Ibidem.
[122] Ibidem.
[123] Gračev M. A., Mokienko V. M., *Russkij žargon. Istoriko-ètimologičeskij slovar’*, (Moskva: Ast-press, 2009).

2.2. The symbology of the Russian criminal tattoos

A specific language is not the only external manifestation of the criminal underworld, since the antiquity tattoos have been employed by different social categories to mark their bodies, as a sign of identification and belonging to a given community. Six thousand years ago the Egyptians used to mark on their skin their titles or qualities, the Greeks and the Romans were imposing tattoos on dominated people, as a sign of submission and surrender and generally we can say that the practice of the tattoos has always been common throughout the centuries and the populations. As observed by Graven[124], the tattoos have been usually associated with the 'primitive', the 'savage' and something not totally human but more brutal and closer to the animal nature. The savage as the criminal are associated by the '*règle générale de l'analgésie*'[125], the deep insensitivity vis-à-vis the sorrow. Within the criminal underworld, the tattoos were and partially still are a sign of distinction, of opposition to the common and shared value of the society, a mark of belonging to a specific group and in the case of the Russian criminals also a chronograph of the criminal's life and a curriculum vitae with mention of characteristics, qualities and specialisations.

In Russia the tradition of criminal tattoos traces back to the Tsarist times, where it was common to physically mark the criminals. According to the research of Baldev, Vasilev and Sidov[126], until 1846 the tattoos '*vor'* ('thief') was applied to criminals condemned to hard labour. There were three main types of brands applied to the right forearm and to shoulder blades: the letters 'SK' which stand for *Ssyl'no Katoržnyj* ('hard labour convict'), 'SP' that refers to *Ssyl'no Poselenec* ('hard labour deportee) and the letter 'B' that stands for *Beglec* ('escapee')[127]. An evolution in the practice of tattoos in Russia occurred with the establishment of the forced labour camps in the Union of Soviet Socialist Republics (1922-1991), where professional criminals emerged, particularly during the Stalinist period (1924-1953). As pointed out by Bronnikov, the tattoos were the manifestation of the unwritten law in the Soviet prison system, where a structured hierarchy was present among the criminals and the tattoos had the value of showing to the other convicts the one's belonging to a given criminal group and his experiences and characteristics. A tattoo had a high value, since they truly represented the owner, as a consequence and individual with fake tattoos was obliged to remove it, by covering it and for this reason, from then on, he was called a 'Blue'[128].

There is an elaborated symbology behind the Russian criminal tattoos, as explained by the research conducted by Etter, Pottorff and Urban[129]. Russian criminals often present tattoos covering their hand and fingers, in particular ring tattoos, each of them representing a specific offense committed by the criminal. The most common tattoos on the hands are: a five dots symbol, representing four watchtowers and a convict; the cat,

[124] Graven J., *L'argot et le tatouage des criminels*, (Neuchâtel: Histoire et Société d'aujourd'hui – Editions de la Bconnière, 1962.
[125] Ibidem.
[126] Baldev D., Vasiliev S., Sidorov A., *Russian Criminal Tattoo Encyclopaedia*, Vol.3, (London: Fuel Publishing, 2014).
[127] Ibidem.
[128] Bronnikov A., *Russian Criminal Tattoo: Police Files*, Vol.1, (London: Fuel Publishing, 2016).
[129] Etter G.W., Pottorff S.N., Urban V.E., *Decoding the Tattoos of the Russian Mafia*, the Journal Gang Research, August 2018.

indicating that the wearer is a *Korennoj Obitatel' Tjurmy* ('Native Prison Inhabitant'); the crosses on the knuckles, which refer to convictions and then different rings tattooed on each finger with a specific meaning[130]. Moreover, the tattoos served also as sign to distinguish the different ranks among the criminals. For instance, two eight-pointed stars on the chest or on the shoulders mean that the wearer is an authority, while the same tattoo on the knees means that the criminal will not submit to the authorities; an eight-pointed star on the upper chest indicates a semi-authority[131]. Other common tattoos were those ones marking the face, which were usually the result of the 'card game of chance' as observed by Bronnikov, where the loser accepted to be tattooed on the face. Facial tattoos include a wide variety of symbols, among which prison bars, swastika, or the words: 'junta', 'Communist Party slave' or 'slave of the zone'[132]. Furthermore, tattoos showing disrespect for the Soviet government were common, among which tattoos with Nazi motives and themes. There were also the so-called 'political tattoos', which had an instrumental value, like those ones representing Stalin or Lenin, which were tattooed over the heart and the vital organs as a form of protection, since during Soviet times icons representing Lenin or Stalin were considered sacred, hence guards would have not shoot a criminal on that part of the body[133]. There are then religious tattoos which symbolise non-religious meaning. For instance, the tattoo of the Madonna means loyalty to the criminal clan; a church surrounded by barbed wire refers to imprisonment and the number of domes on the church symbolises the number of convictions of the wearer. There are also anti-Semitic and anti-Islamic tattoos, which often are completed by Slavophile or nationalistic expressions. There are then specific tattoos indicating the criminal offenses committed by the criminal, for example, the spiders were often used to underline the commitment and dedication of an individual to the criminal life, while nowadays they represent involvement into the drug business; the tattoo of two bells rung indicates that the criminal does not cooperate with the authorities; the pirate refers to a conviction for robbery; the ants, beetles, bumblebees, cockroaches and flies are the symbols of pickpockets; the skull pierced by a knife or completed by crossbones represents a murder; a bear refer to a professional safecracker. There were also a set of tattoos to stigmatise individual not deserving respect within the criminal community such as informers, those which broke the criminal rules, those stealing from other criminals, former police officers, sex offenders and homosexuals.

In the aftermath of the dissolution of the Soviet Union in 1991, the practice of criminal tattoos has weakened, nevertheless it is a still alive tradition among Russian-speaking criminal groups. Moreover, after 1991, several Russian criminals have emigrated abroad and once in prison, have maintained the old traditions and rules, among which that one of the prison tattoos, which spreads then outside the Russian Federation as well, and this is why knowing the meaning of these marks is useful on the one hand to recognise the roles and hierarchy of a criminal and on the other side, to have a wider and more comprehensive knowledge about the Russian criminal phenomenon. The habits, outlook and methods of *Rossijskaja Organizacija* may have changed

[130] Ibidem.
[131] Ibidem.
[132] Bronnikov A., *Russian Criminal Tattoo: Police Files*, Vol.1, (London: Fuel Publishing, 2016).
[133] Etter G.W., Pottorff S.N., Urban V.E., *Decoding the Tattoos of the Russian Mafia*, the Journal Gang Research, August 2018.

throughout the years, but specific traits of the original mentality based on honour, ruthlessness and the strive for power have persisted unchanged. Therefore, if the intent is to counter the threat placed by these groups to the security architecture of Europe, it is essential to know them deeply and understand where do they come from, because we cannot truly comprehend something if we do not look back at its origin.

III. THE *ROSSIJSKAJA ORGANIZACIJA* AND ITS INFILTRATION IN EUROPE

1. The threat of the *Rossijskaja Organizacija*

According to Ulrich Beck[134] the most characterising factor of contemporary society is the perception of the risk and its management. According to the German sociologist we are living in a "new modernity" where the nation-state alone cannot satisfy the request of security of its own citizens. Beck, in his theory of the "risk society", initially, elaborates mostly on the effects of globalisation on the society and of the technological advancement and relative harms. Nevertheless, his theory has a wider breath and can be applied to contemporary society as a whole, in its different domains (political, economic, cultural, scientific). Moreover, what it is underlined by Beck, is the fact that the risk in the globalisation era cannot be handled individually by a country but necessitates coordination among the different parties involved, since its nature in contemporary society is transnational. The perception of the risk and the need to minimise it characterise our society and it is an issue that governments, law enforcement authorities and intelligence agencies must handle in order to guarantee security. The increase perception of an uncontrollable risk marked the European continent after the fall of the Iron Curtain and the collapse of the Soviet Union. Within the European Community (later European Union, 1993) a feeling of insecurity permeated the society, threatened by the opening of the Eastern borders and the increased movement of people coming from the Eastern bloc. Among the changes introduced by these historical events, that one related to the perception of organised crime in Western Europe is of interest for the present research. As analysed by Fijnaut and Paoli[135], before the turning point in history of the last two decades of the twentieth century, aside from Italy, all other European countries considered themselves to be unaffected by the threat of organised crime. This perception changed drastically in the aftermath of the aforementioned historical events. Among the main reasons, the capillary spread westward of the illegal drug industry from the East and the related consequences to the Western European societies, that played a pivotal role in the construction of a new perception and the genesis of the organised crime's paradigm in Europe. In particular, significant attention was placed on the emergence of a specific type of organised crime, the *Rossijskaja Organizacija*. Experts and sovietologists were extremely concerned by this new form of threat, which was seen as a continuation of the "empire of evil" in another form. The *Rossijskaja Organizacija* was perceived as equipped with all those characteristics typical of the Soviet Union, such as the strive for power, expansionism, brutality, lack of scruples and technological knowledge. A new threat was emerging, which the West was not prepared to handle and new risks were placed to the European security architecture, risks that are still vital and dangerous for Europe. In order to manage these risks, we need to know the adversary, the other side, we need to understand how its mind works, which reasons and emotions move its actions, which

[134] Beck Ulrich, *Risk Society. Towards a New Modernity*, (London: Sage, 1992).
[135] Fijnaut Cyrille and Paoli Letizia, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004).

believes permeate its society, how they speak and elaborate about themselves and the "others". To capture the features and strategies of the *Rossijskaja Organizacija* it is essential to look at its roots and development in Russia and then its expansion westward. Moreover, to understand it and effectively counter the threat placed to the European security we need first to understand the society and the context in which it emerged. “Russia cannot be understood with the mind alone”, stated in the XIX cent. Fëdor Ivanovič Tjutčev, Russian poet and statesman. If we truly want to understand how Russian criminals work, which are their objectives and targets, which will be their future development, a deep and multidimensional approach to the Russian society, culture and politics is essential, covering not just one aspect but different layers of analysis: historical, cultural, linguistic, economic, political and sociological. If we aspire to guarantee security in the European Union and minimise the risk placed by external threat actors, it is indispensable to know and understand our enemy.

2. Problems of terminology

The terminology employed in the present research to describe the phenomenon of organised crime linked with Russia is ‘*Rossijsakaya Organizacija’*. Before describing the reason behind this terminological choice, a brief overview of the terminologies proposed is needed. The phenomenon of organised crime with connections to Russia is a contested concept in terms of definition and terminology and there is no consensus on a single and unambiguous term to describe it. Sometimes are used the terms *Rossijskaja mafija* or *Russkaja mafija*[136] (both generally translated in English as ‘Russian mafia’) to describe it. There is a relevant *nuance* in the two expressions, that is possible to capture only in the Russian language, since it has not equivalent, at least in English. The Russian word *русский* (*russkij*) describes something ethnically Russian, e.g. *russkij jazyk* (Russian language), *russkij čelovek* (Russian person); while the word *российский* (*rossijskij*) refers to something belonging to Russia, e.g. *rossijskoe pravitel’stvo* (Russian government), or *rossijskaja armija* (Russian army). So here the dividing line, expressed by the richness of the Russian language, is between the ethnicity *(russkij)* and aspects related to the belonging to the State (*rossijskij*)[137]. A further term needs to be explained in relation to the concepts of “nationality” and “ethnicity”. In the Russian language a clear distinction – that is not evident in other languages – is that one between the term *россиянин (rossijanin)*, which means “citizen of the Russian Federation” and *русский (russkij)* which refers, as pointed out by the Russian political scientist and philosopher Aleksandr Dugin[138], to something deeper, which is not related to a choice, but to the bond of blood, ethnicity. This clarification about the terminology employed in Russian-speaking context is fundamental to understand the organised crime linked to Russia, since the language is not

[137] Nikonov Vyacheslav, “Russkij Mir: Cmysly i Cennosti” Ch.3 in *Cmycly i Cennocti Russkovo Mira. Sbornik statej i materialov kruglych stolov, organizovannych fondom «Russkij mir»*, (Moskva: Fond Russkij Mir, 2010).
[138] Dugin Aleksandr Gel'evič, *Russkij Logos – russkij Chaos. Sociologija russkovo obščestva*, (Moskva, Akademičeskij proekt-Gaudamus, 2015).

neutral and it implies always different meanings and relevant *nuances*. Other times the term *Bratva* ('Brotherhood') is employed to describe organised crime linked to Russia. In this case as well, further explanation is needed. As highlighted by Krivova[139], during the twentieth century the use of the term '*bratva*' had not a negative meaning. The pejorative sense of the term was the result of its usage in jargon and the negative stigmatisation given by the society, the outside. In fact, the term '*bratva*' was employed with the meaning of '*druz'ja – soobščniki'* (comrades-accomplices) and '*sokamerniki*' (cell mates) in the prison slang, while in the criminal language it refers to '*mafioznye gruppy*' (Mafia groups). The same goes for another related term, *'bratok'* (colloquial: brother, friend, associate) which emphasised the belonging to the fraternity or brotherhood, namely *bratstvo*[140]. Another way to define organised crime linked with Russia is '*Organizovannaja Prestupnaja Gruppa'*, usually shortened with the acronym OPG, which means literally 'Organised Criminal Group'.

Moreover, the problem of definition and even terminology of organised crime linked with the Russian Federation is discussed by Galeotti[141] as well, and the scholar suggests to use the term Russian-based organised crime (RBOC) to define the phenomenon, since this term focuses on the exposure to Russia and not on ethnicity or language. A plethora of terms have been used to describe the phenomenon, but none of them describes in a complete and accurate way the object in question. Notably, the terminology of "Russian organised crime" does not recognise the engagement of a number of other ethnicities, such as the Ukrainians or the Georgians; while, "Russian-speaking organised crime" is considered to be inaccurate since criminal from ethnicities other than the Russian one may use their own language alongside with the Russian language. Another terminology employed is that one of "Eurasian organised crime", that, if it is complete in terms of actors involved, it is quite inaccurate at the same time, since it involves too many groups and phenomena. The terminology proposed in this research is that one of "*Rossijskaja Organizacija*", since I believe it is the most accurate for different reasons. This syntagma describes accurately the nature of organised crime linked to Russia, in fact the term '*rossijskaja*', as explained above, refers to something belonging to Russia, without necessarily being ethnically Russian. On the other hand, the second term of the syntagma, namely "*organizacija*", is more accurate of other terms proposed such as "groups" or "mafia", the first being to generic and the second just inaccurate. In fact, according to the present research, the phenomenon of the '*Rossijskaja Organizacija*' outside Russia, as it will be further explained, cannot be completely associated with that one of "mafia". On the one hand, *Rossijskaja Organizacija* shows common characteristics, methods and purposes of mafia groups but, on the other, it lacks specific requirements, to be categorised as "mafia".

[139] Krivova N.F., *Kategorija social'noj ocenki v gruppe suščestvitel'nych so značeniem lica,* Lingvistika Vestnik Nižegorodskovo universiteta N.M. Lobačevskogo ,2010, № 4 (2), c. 572–574.

[140] Dictionary for Russian jargon employed: Mokienko V.M., Nikitina T.G., *Slovar' Žargona – Bol'šoj Slovar' Russkovo Žargona*, SPB, 2000.

[141] Galeotti Mark, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, European Council of Foreign Relations, April 2017.

2.1. Mafia and Rossijskaja Organizacija

The *Rossijskaja Organizacija* shares common characteristics with mafia groups, hence the label employed by part of the literature of "Russian Mafia". Nevertheless, according to the present research, Russian organised crime cannot be completely associated with mafia-like groups, hence the adopted terminology is *Rossijskaja Organizacija* (hereafter: *RO*). In fact, as observed by Finckenauer and Waring, Russian organised crime lacks of the high-degree of centralisation and tight hierarchical structure typical of conventional mafia networks, rather it presents a fluid nature[142], that involves a variable geometry in terms of composition with no fixed members, rather occasional groups coming together to perpetrate a given criminal operation. There is, in the Russian context, a trend towards a more horizontal rather than vertical organisational hierarchy. Another relevant aspect which distinguishes *RO* and mafia is the role played by familial ties, which are not substantial in shaping Russian criminal networks. Familial ties and common ethnicities are specific features for example of the Colombian, Italian and Mexican mafias operating abroad; while, considering the *RO*, the links with family and ethnicities are just a secondary issue, since, as pointed out by Finckenauer and Voronin, the main driver for the building of the network relies just on the shared interest in criminal activities and the mutual benefits thereof[143]. Furthermore, the notion of mafia is typically associated with the Italian criminal groups and their specific traits, influenced and rooted in the national context where they were born. The Sicilian mafia, for instance, is linked to some specific aspects, traditions and customs of the Sicilian history, which have been instrumentally employed and distorted in their application to criminal activities. Virtuous concepts of respect for the family and honour, traditionally rooted in the Sicilian tradition and history, have been employed and manipulated by the Sicilian mafia to build its identity, alongside with other concepts like the code of silence (*omertà*), which all have contributed to delineate the boundaries of the mafia concept, which differs substantially to the characteristics of the *RO*.[144] Nevertheless, there are some aspects in which *RO* and traditional mafias are alike, namely in the service they provide, that is protection. As observed by Varese[145] as well as Gambetta[146], the mafia is essentially a protection and security provider that meets the demand of the citizens of an inefficient State unable to provide such services. In this sense the *RO* can be partially ascribed to the mafia paradigm, since it has taken advantage of the failure of the State in the transition towards capitalism, substituting the State in the process and acting as a rational actor in the economy, as illustrated by the rational choice theory (hereafter: RCT). This theory has been applied to organised crime and mafia groups by Shvarts, specifically to the Sicilian mafia and Russian organised crime, concluding that there is an analogy between the two groups. Notwithstanding the excellent work conducted by Shvarts, the present research

[142] Finckenauer James O., Waring Elin J., *Russian Mafia in America*, (Boston: Northeastern University Press, 1998). pp. 202-229.
[143] Finckenauer James O., Voronin Yuri A., *The Threat of Russian Organized Crime*, Issues in International Crime, NCJ 187085, June 2001.
[144] Finckenauer James O., Waring Elin J., *Challenging the Russian Mafia Mystique*, National Institute of Justice Journal, April 2001.
[145] Varese Federico, *The Russian Mafia. Private Protection in a New Market Economy*, (Oxford: Oxford University Press, 2001).
[146] Gambetta Diego, *The Sicilian Mafia. The Business of Private Protection*, (Harvard: Harvard University Press, 1993).

disagrees with that conclusion and considers the *Rossijskaja Organizacija* as a phenomenon of different nature from mafia, essentially because of his structure and organisational patterns. However, it is recognised the value of the aforementioned research conducted by Shvarts with respect to the application of the rational choice theory to Russian organised crime groups, that highlights the high-level of professionalism and penetration of the *RO* within the economical and societal tissue, but the application of the model to both Sicilian mafia and Russian organised crime, is not considered in the present research, as a proof of the analogy of the two terms. Therefore, considering rational choice theory (RCT), the criminal is a rational individual that sets in place a cost-benefits analysis for his or her criminal activities and in the case of Russian criminals, due to the nature of the dysfunctional state and pervasive corruption at the economic and political level, the benefits outweigh generally the costs and this is one of the main reasons of the spread and development of a new form of organised crime in the Russian Federation in the post-Soviet era.

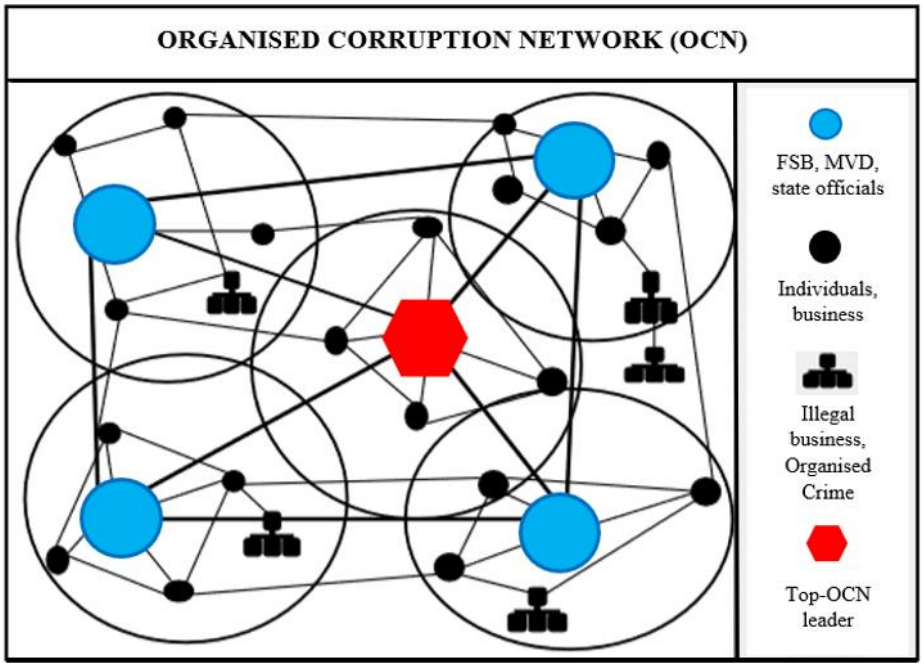
3. Dysfunctional State and *Rossijskaja Organizacija*

The emergence of the *Rossijskaja Organizacija* was both a result of the imperfect transition of the Russian Federation from a state-run to a market economy in the aftermath of the fall of the Soviet Union in 1991 and a product of the globalised world. As observed by Armao[147], the globalisation has caused the deconstruction of the State, that has lost its centrality, and has created a wide range of new opportunities for organised criminal groups, through the deregulation of the financial markets and the wave of privatisation. These phenomena joint together have opened the way to the establishment of a crime-building process, particularly in those states with weak governance and legislation, such as the Russian Federation. However, as discussed in chapter II, contemporary Russian criminals trace their origin back to Tsarist Russia and in particular to the emergence of the *vory v zakone* (thieves-in-law) in the Stalinist Gulag system. Nevertheless, throughout the decades, the profile and characteristics of the criminal underworld in the Russian Federation underwent substantial changes, which led to a new category of criminals with few in common to the original "fathers". Therefore, to understand the contemporary outlook of Russian criminal groups and their organisation and purposes, it is necessary to consider the last decades of the twentieth century and the evolution from that point on.

[147] Armao Fabio, *Criminal Clusters: State and Organised Crime in a Globalised World*, The European Review of Organised Crime 1 (1), 2014, 1-44.

During those years the Russian state proved to be unable to cope with the challenges posed by the transition on different level of analysis, among which, most prominently in the legal and economic ones. The legal situation in the Russian Federation in the aftermath of the collapse of the Soviet Union was characterised by a chaotic and disorganised set of overlapping laws and decrees and the tax system was suffering of the same inefficiency. This inability of the State to create an optimal environment for a successful transition towards a market economy, triggered a widespread and unregulated struggle in the privatisation of the assets, leading to the emergence of a class of powerful individuals, which were able to grab most of the initial distributed resources and property rights. As observed by Varese, when a state is unable or unwilling to define and protect property rights, two main effects are produced.

Fig. 1



Source: author's elaboration based on Cheloukhine Serguei, Maria Haberfeld, *Russian Organized Corruption Networks and their International Trajectories*, (New York, Dordrecht, Heidelberg, London: Springer, 2011).

The first is a decrease in the demand of protection of property rights by the state, while the second will be the rise of corruption, due to the fact that individuals will try to enhance and protect the value of their assets[148]. The main beneficiaries of the Russian transition were a class of enterprise managers, which were able to benefit of the transfer of resources by taking advantage of controversial privatisation auctions and emerged as the so-called Russian "oligarchs"under the presidency of El'cin (1991-1999)[149]. In the late 1990s enterprises, banks and commercial services were subjected to a criminal system of protection called *kryša* ('roof') or *silovoe partnerstvo* ('enforcement partnership'), due to the lack of functional law enforcement authorities. A *kryša*

[148]Varese Federico, *The Russian Mafia. Private Protection in a New Market Economy*, (Oxford: Oxford University Press, 2001).
[149] Freeland Chrystia, *Sale of the century: Russia's wild ride from communism to capitalism*, (New York: Crown Publishers, 2000).

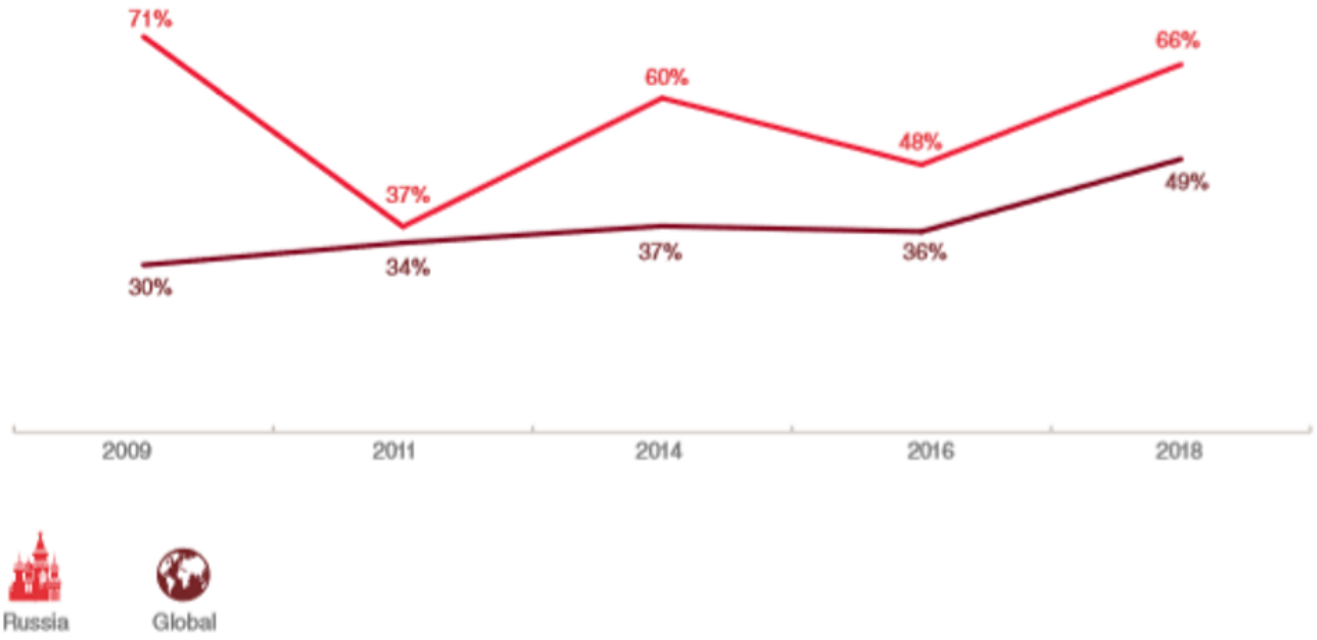
was a guarantee of protection of a business, which relied on the influence of a given criminal group, to which a payment was made as percentage of the profits of the activity, that acted as a protector, deterring other criminal groups to exercise exploitation on the activity. According to Volkov, the majority of high-level business transactions and agreements were possible only if an 'enforcement agreement' was concluded, having as contractors the company on the one side and criminal groups or the security services on the other[150]. This system, originated in the late 90s, is still alive in contemporary Russia and it allows the *Rossijskaja Organizacija* to grow exponentially in terms of financial capacity and influence over the state economy. For instance, Volkov reported that the Moscow-based *Podol'skaja* organised criminal group, was able to raise up to US$303 million dollars, through a partnership with a food import firm called Sojzkontrakt. In the late 90s the *modus operandi* of the *Rossijskaja Organizacija* changed drastically evolving from the extortion (*polučat'*, 'to collect') and control of financial transactions (*kontrolirovat'*, 'to control') to a model of full integration within the business controlled, by holding the majority of the shares of the same business (*byt' v dole*, 'to hold a share'). In this way the 'old' *avtoritety* began to be known as businessmen[151]. Examples of this change in the role of the *Rossijskaja Organizacija* in the economic domain are represented by the cases of the *Uralmaš* and *Tambovskaja* criminal groups. The former was a criminal group operating in the 1980s in Ekaterinburg, mainly through extortion and racket and by means of ruthless violence and intimidation. In the 90s the same group exploited the opportunity presented by the transition to the market economy and evolved into a more sophisticated criminal group, deeply involved into business transactions and investments, establishing more than 200 companies, 12 banks and holding shares of 90 companies[152]. The second example is represented by the *Tombovskaja* criminal group, active in Saint Petersburg, mainly in racketing, which turned in the 90s to the legal economy and became involved in the fuel trade.

Moreover, Cheloukhine and Haberfeld, have studied the phenomenon of corruption in the Russian state and have underlined the presence of an organised corruption network (OCN) composed by members of a family that occupied the most prominent positions of governmental structures like the MVD (*Ministerstvo Vnutrennikh Del;* Ministry of Internal Affairs of the Russian Federation), Federal Customs Service, FSB (*Federal'naja služba bezopasnosti Rossijskoj Federacii*; Federal Security Service of the Russian Federation), Central Bank, and several municipal administrative bodies. The leading personalities of the OCN were tasked with the management and supervision of the operations and with the establishment of close relations with the federal political authorities; members of the MVD were assigned to the illegal labour market and immigration; FSB officers gathered intelligence to guarantee the protection of the members of the OCN, while members of municipal administration handled the management of business registration and licences[153]. Therefore,

[150] Volkov Vadim, "The Russian Mafia: Rise and Extinction", Ch.7 in *The Ofxord Handbook of Organized Crime*, edited by Letizia Paoli, (Oxford, New York: Oxford University Press, 2014).
[151] Volkov Vadim, "The Russian Mafia: Rise and Extinction", Ch.7 in *The Ofxord Handbook of Organized Crime*, edited by Letizia Paoli, (Oxford, New York: Oxford University Press, 2014).
[152] Ibidem.
[153] Cheloukhine Serguei, Maria Haberfeld, *Russian Organized Corruption Networks and their International Trajectories*, (New York, Dordrecht, Heidelberg, London: Springer, 2011).

organised criminal group through extensive and pervasive OCN are able to control companies in different sectors and levels of the economy. Moreover, as pointed out by the research conducted by Cheloukhine and Haberfeld, there is a high-degree of specialisation within the criminal groups, each focusing on a specific domain and coordinating with others on a tactical-level. The widespread penetration of the *Rossijskaja Organizacija* in the economy of the Russian state is also acknowledged by the PricewaterhouseCoopers Russian Economic Crime and Fraud Survey 2018[154], that shows an increase in economic crime in Russia from 2016 to 2018, with asset misappropriation, bribery and corruption and procurement fraud as the top ranking crimes committed. Corruption is a "key enabling factor" for organised crime[155], that allows the smooth deployment of the primary criminal activities both in the public and private sectors, with the integration of high-level officers or managers in the illegal network. In fact, as reported by the research of PricewaterhouseCoopers, most of the economic crimes in the private sector are perpetrated through the participation of a corrupted company management (39% of internal perpetrators are senior managers).

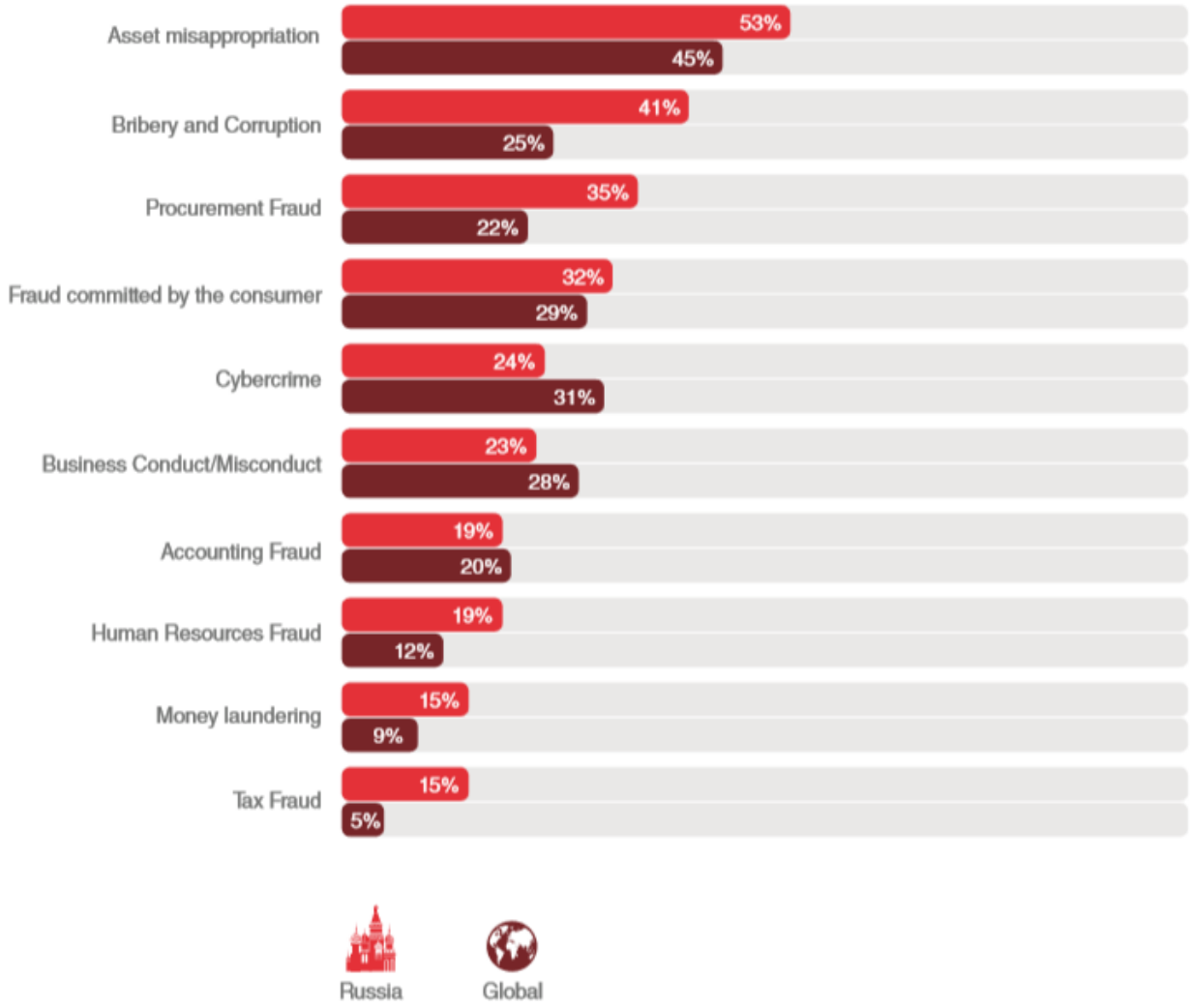
Fig.2 Reported rate of economic crime in Russia and globally



Source: PricewaterhouseCoopers, *Russian Economic Crime and Fraud Survey 2018. Combating Fraud: measures taken by companies*.

[154] PricewaterhouseCoopers, *Russian Economic Crime and Fraud Survey 2018. Combating Fraud: measures taken by companies*. Available at: https://www.pwc.ru/en/forensic-services/assets/PwC-RECS-2018-eng.pdf.
[155] Keene Shima D., *Silent Partners: Organized Crime, Irregular Groups, and Nation-States*, Strategic Studies Institute and U.S. Army War College Press, U.S., October 2018.

Fig.3 Main types of economic crime in Russia and globally



Source: PricewaterhouseCoopers, *Russian Economic Crime and Fraud Survey 2018. Combating Fraud: measures taken by companies*.

A turning point has been the accession to power of Vladimir Putin, which became for the first-time president of the Russian Federation in 2012 and nowadays in his fourth term of office. In fact, under the presidency of the strong man of the Kremlin, the linkages between the State and criminal groups have been exploited to the benefits of the former. A process of "nationalisation" of the underworld has taken place, as observed by Galeotti, with former criminals enrolled in the top political and economic spheres and a "gangsterisation" of the formal sectors, with the use of violence and intimidation[156]. Putin has exercised a tight grip over the corrupted Russian economy but with the aim of imposing control, handle it and subdue it to the centralised state. As a matter of fact, under Putin the powerful and corrupted economic establishment, composed by the so-called oligarchs, was deposed. Nevertheless, the result was not a decrease in the overall level of corruption, rather an increase of corruption, in particular within the judicial system, disproportionally complaisant towards

[156] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven, London: Yale University Press, 2018).

the President's actions and decisions[157]. The change introduced by the president Putin was called the *vertikalnaja sistema* ('vertical system'), which refers to the process of partial nationalisation of the main industrial sectors, the energy sector in particular, which are strategically fundamental for the Russian Federation. With the establishment of this new system, as observed by Karpanos[158], the oligarchs were compelled to agree on a new type of cooperation with the State, based on the redistribution of political and economic power. The fallout was that by 2012 Russia's main strategic companies (such as Gazprom, Rosneft, Sukhoi, Sberbank and United Energy Systems) were partially controlled by the State, which replaced the oligarchs with civil servants and Putin's personal linkages. The *vertikalnaja sistema* established from the 2000s had consequences on the Russian organised crime groups, since the new system absorbed criminals into state institutions on the one hand, and on the other it led many of the 1990s oligarchs to move abroad, where they continued to manage their business, relying on the same methods adopted at home, namely the connections with the criminal underworld, thus increasing the level of criminal activities carried out in Europe. Moreover, a key of interpretation of the aforementioned scenario is that one of the 'Muscovite paradigm' offered by Caselli[159], according to which the power exercised by the zar/president over the property rights and the economy is absolute and the functioning of the economy is based on the network of relations between the state authority on the one side and the interest groups on the other, which are subjugated to the Kremlin. The contemporary Russian state is a dysfunctional organism, whose shortcomings and deficiencies are partially attributable to the Soviet legacy and to the transition to a market economy. In particular, the Russian state is characterised by an endemic political, institutional and economic weakness, all conditions which favour the criminal-governmental nexus and the continuation of a system of power based on personal relations and agreements with the influential actors in the scenario such as politicians, businessmen or criminals.

3.1. The role of the Russian Intelligence

The *liaison*, between the organised crime on the one hand and the dysfunctional state apparatus on the other, has consequences also on the world outside Russia, when crime groups are transplanted abroad or when specific operations are directed outside the boundaries of the Russian Federation. Indeed, the exploitation of the *Rossijskaja Organizacija* by the state security services has been widely acknowledged. As observed by Galeotti, there is a growing evidence of contacts between the criminal groups and the Russian security agencies, particularly the Foreign Intelligence Service (SVR), the Federal Security Service (FSB) and the military intelligence (GRU)[160]. What is relevant for the European security system is the evidence that Russia

[157] Benvenuti Francesco, *Russia Oggi. Dalla caduta dell'Unione sovietica ai nostril giorni*, (Roma: Carocci editore, 2013).
[158] Karpanos Ilona, *The Political Economy of Organised Crime In Russia: The State, Market and Criminality in The Ussr and Post-Soviet Russi*a, (London: Department of International Politics, 2017).
[159] Caselli Gian Paolo, *La Russia Nuova. Economia e Storia da Gorbačëv a Putin*, (Milano, Udine: Mimesis Edizioni, 2013).
[160] Galeotti Mark, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, European Council on Foreign Relations, April 2017.

is employing the *Rossijskaja Organizacija* as a tool of the Kremlin's geopolitical agenda to undermine the West, through covert and indirect operations[161]. There have been, according to Galeotti, a vertical integration of the organised crime, that has become "an instrument of statecraft abroad"[162]supposed to comply with the requests made by the Kremlin. Evidences of the connections between organised crime and the intelligence agencies are clearly visible in the cyber-attacks conducted against Western targets and perpetrated by the APT28 (also known as 'Fancy Bear') associated with the military intelligence agency (GRU) and APT29 (also known as 'Cozy Bear') supposedly link to the Federal Security Service (FSB). Alongside with the cyber domain, Russian criminal resulted to cooperate with the state's security apparatus in other activities, among which the raise of 'black account' funds (*čërnaja kassa*) to finance political operations in Europe, gathered mainly through smuggling activities and that cannot be traced and can be used more easily than funds located in Russia. Another way in which the Russian security services exploit the *Rossijskaja organizacija* is through the use of the so-called agents of influence, criminals well integrated in the business community as investors or brokers, which are sent abroad to exert political influence and gather information. One of the several examples of this kind of operations handled by the Russian intelligence services is that one of Evgenij Burjakov, officially working for an investment company (VEB.RF, ex-Vnešèkonombank) and arrested in New York in 2015 for being an officer of the Foreign Intelligence Service (SVR)[163]. A more recent case is that one of Alexander Koršunov, top manager of the United Engine Corporation (UEC), a Rostec's subsidiary, that has been arrested on 30th August 2019 in Naples by the Italian authorities under request of Washington, with the accuse of industrial espionage against the United States of America[164]. Organised crime groups are also employed by the security services for moving people and goods across borders without being noticed, as in the case of a Russian agent, Christopher Metsos, discovered by an FBI operation in 2010. Russian state security agencies are also supposed to exploit their connection with the criminal underworld to order assassination, as testified by the case of Alexander Litvinenko, killed in London in 2006, or the more recent Skripal case on 4th March 2018, where a former Russian military intelligence officer and double agent for the UK's intelligence services, was poisoned in Salisbury, England[165]. Moreover, as reported by the Swiss Federal Office of Police[166], there are evidences of the cooperation between the *Rossijskaja Organizacija* and the Russian intelligence in Europe, particularly in Germany and Switzerland. In the latter, the Swiss Federal Office of Police assumes that Russian security services and organised crime groups deploy their agents to Swiss-based

[161] Galeotti Mark, *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations, May 2016.
[162] Ibidem.
[163] Galeotti Mark, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, European Council on Foreign Relations, April 2017.
[164] Vedmosti, *Top-menedžera «dočki» «Rostecha» zaderžali v Italii po zaprosu SŠA. Ego podozrevajut v èkonomičeskom špionaže*, 05 September 2019. Available in Russian at: https://www.vedomosti.ru/politics/articles/2019/09/05/810548-zaderzhali-italii?fbclid=IwAR2mc-jDiDWLrtfxbmL2Qwfd5m-ol93iWNfmzFdT23zye-8-VfUs1ErzrDY.
[165] Juurvee Ivo, *The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox*, Strategic Analysis, April 2018.
[166] The Swiss Federal Office of Police – Service for Analysis and Prevention, *Strategic Analysis Report: Organised Crime and the Special Services of the Commonwealth of Independent States*, June 2007. Available at: https://tbcarchives.org/fsb-and-organized-crime-connection-analytical-report/.

companies for money laundering activities. Furthermore, the aforementioned report affirms that "Switzerland is in the focus of attention of Russian security services" and this is testified by the presence in the country of the second highest number of Russian high rank staff stationed in Switzerland (after Germany) among Western European countries. According to the Swiss analysis around 75% of Russian intelligence officers work in Geneva under diplomatic cover and as employees of the international organisations based in the city. According to the analysis conducted by the Swiss in 2007 there were around 700 Russian companies in Switzerland, 60% based in the German-speaking part and approximately 34% in the Western part of the country, some of these enterprises were headed by former Russian security officers and the employees resulted to have connections with the Russian Intelligence or former officers of the KGB[167].

4. The spread of the *Rossijskaja Organizacija* in Europe

The implantation of the *Rossijskaja Organizacija* in Europe began during the 1970s with the Jews emigration agreement signed by the Soviet Union and the United States of America. As reported by Kegö and Molcean about 291.000 Jews emigrated from the Soviet Union, most of them indicated as destination countries the United States and Israel, but a significant part actually settled in Europe, especially in Germany. Moreover, in 1988 another wave of emigration from the Soviet Union was directed towards Europe, composed mainly by Armenians (56.500) and ethnic Germans (322.000)[168]. Among the emigrants from the Soviet Union, there were a number of individuals with criminal records, which gave birth to organised criminal groups within Europe. Nevertheless, as stated before in the present research, the turning point in the presence of the *Rossijskaja Organizacija* in Europe, was represented by the fall of the Soviet Union at the beginning of the 1990s and the subsequent transition to the market economy. In fact, the transition process coupled with the globalization opened a wide window of opportunities for the economic development of countries as well as for criminal activities. Movements across borders became easier and the contacts among criminal groups based in different countries increased. Moreover, in the post-Soviet era a number of organised criminal groups operating in Russia decided to move abroad, especially in Europe for a number of reasons, among which the threat of internal fights among criminal groups within Russia, prosecution by law enforcement authorities or as a result of a planned operation designed by Russia's intelligence services. Indeed, according to the so-called theory of "controlled expansion of organised crime", sustained by the U.S. intelligence, behind the massive emigration of criminals from the Soviet Union there was a plan of the KGB. Evidences of this theory would be the fact that several members of organised crime group coming from the Russian Federation, were trained and assisted to move abroad by the KGB[169]. Particularly exposed to the threat of the *Rossijskaja Organizacija* are Germany and the North-eastern part of Europe, where the Russian criminal groups are involved mainly in

[167] Ibidem.
[168] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011).
[169] Ibidem.

money laundering operations for activities carried out in Russia or in the former Soviet Republics. Nevertheless, organised crime transplantation requires a number of conditions which are difficult to be satisfied, exposed by Reuter[170] and Gambetta[171] as follows: the ability to monitor agents, that is made harder due to the distance; the collection of information, that is complicated by the lack of a trusted network; the reputation, that requires long-term relations. Therefore, a transplantation of a criminal network requires a cost-benefits analysis, where the latter outweighs the former in order to be successful. Varese[172] analyses the factors facilitating the transplantation of an organised crime group, among which the most relevant is the generalised migration in the target territory from the country of origin of the organised crime group. Nevertheless, a transplantation to be successful requires other elements, which are summarised by Varese[173] in two categories: the supply and the local conditions significant to demand. As far as the supply is concerned, the necessary elements for the transplantation of an organised crime group are the presence of resources in the destination country, namely labour force, available counterfeited documents, bank accounts and technical equipment such as arms and spying technology. Another factor that is relevant on the supply-side is the possibility of informal investments and money laundering, alongside with the presence of a profitable market sectors with few competitors. On the demand-side, the relevant factors for a successful transplantation according to Varese are the level of trust towards the institutions and civic engagement in the destination country, (the lower the levels of the aforementioned elements, the higher the chance for a successful transplantation); the need of criminal protection for illegal activities; the size of the market, where a local dimension is preferable for the transplantation of an organised criminal group, due to the possibility to monitor the agents, collect reliable information and gain a valuable reputation.

As far as the presence and transplantation of the *Rossijskja Organizacija* is concerned, in the following sections will be provided an outlook of the main characteristic of the *Rossijskaja Organizacija* in the destination countries within the European Union –with a specific focus on Germany, Italy and the Baltic countries – as well as an in-depth analysis on the money laundering activities.

4.1. Main characteristics

The *Rossijskaja Organizacija* does not present a homogenous character, nor within the Russian Federation, neither outside it. As analysed by Kegö and Molcean[174], different classifications of the phenomenon can be provided with some groups active in Europe that can be classified as presenting themselves with a hierarchical

[170]Reuter Peter, *The organization of illegal markets: An economic analysis*, (Washington: U.S. National Institute of Justice, 1985). pp. 7-24.
[171] Gambetta Diego, *The Sicilian mafia: The business of private protection* (Cambridge MA. Harvard University Press, 1993). pp. 246-251.
[172] Varese Federico, *Mafias on the Move. How Organized Crime Conquers New Territories*, (Princeton, Oxford: Princeton University Press, 2011). pp. 13-30.
[173] Ibidem.
[174] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp.22-28.

structure, as loose affiliations or semi-autonomous and independent gangs with different leaders. What is relevant is also the dynamic nature showed by the *Rossijskaja Organizacija*, with groups able to change their internal organisation, such as the *Solncevskaja* network, that passed from a hierarchical to a loose affiliation paradigm. Another classification is that one stressing the belonging of the Russian criminals to the *vory v zakone* old community on the one hand, which are bound by the Criminal Code and are involved in wide range of activities among which notably money laundering operations and, on the other, those which do not share the belonging to the original Russian criminal underworld and are generally involved in small-scale illegal activities, showing a higher degree of violence employed and a less structured organisation, if compared with the former. Another categorisation is also that one focusing on the country of residence, which distinguishes among: groups based in Russia and former Soviet Republics; intermediary-moving groups and EU-based groups. All these groups operate in Europe, but at different levels. In fact, the groups based in the EU are active on the operational level, given the strong ties with the territory (citizenship or permanent residence permit) and are based mainly in the Baltic countries and Germany due to historical immigration; the groups based in Russia or former Soviet Republics are involved in the decisional and planning levels, while the intermediary groups are engaged in delivery and auxiliary operations.

As far as the characteristics and *modus operandi* of the *Rossijskaja Organizacija* in Europe are concerned, a relevant aspect to underline is the ability to infiltrate the legal economy (particularly the financial and banking sectors), thus investing in businesses and having a legal coverage for money laundering activities. Another feature is the systematic and extensive use of physical violence and intimidation, more than other organised criminal groups, not only within the group or against other competitor groups[175]. Moreover the *Rossijskaja Organizacija* results to be involved in high-level crimes, mainly in the financial sectors, and to keep a low-profile, having low-levels of interaction with the local community where they operate for two main reasons: firstly, for the nature of the crimes committed which does not necessitate tied connections with the locals; secondly, because it makes them less traceable by the law enforcement authorities.

Considering the illegal market of activity, the *Rossijskaja Organizacija* results to be more dynamic than other organised crime groups, being involved in several criminal activities both in the legitimate and illegitimate economy. Nevertheless, as observed by Shelley[176], the *Rossijskaja Organizacija* is mainly involved in the financial and banking sectors, the luxury market, import-export businesses, real estate, transportation, hotels and restaurants, casinos and nightclubs. Moreover, due to the high level of expertise in the hi-tech sector, another domain where there is a pervasive involvement of organised crime linked to Russia is the cyber domain (for an in-depth analysis see ch.4). The main reason why the *Rossijskaja Organizacija* is deeply involved in the legitimate economy relies on the possibility offered to move freely "black money" from Europe to other

[175] Ibidem.

[176] Shelley Louise, "Contemporary Russian Organised Crime: Embedded in Russian Society" in Fijinaut and Paoli, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004). pp. 563-584.

countries of activities outside the European borders, among which Russia, and to provide money laundering operations for other organised criminal groups[177].

As far as the involvement in the illegitimate economy, the Russians specialised in Europe in the following fields: illegal drug trafficking, illicit trafficking of firearms, human trafficking. Considering the drug market, the *Rossijskaja Organizacija* holds a dominant position in the European heroin market, cooperating also with other organised crime actors, mainly with Colombian, Chinese and Japanese groups. The main route of the heroin trade orginates in Afghanistan, passes through Central Asia countries and then get through the whole Russian Federation, following the itinerary of the Trans-Siberian railroad from Moscow to Vladivostok. The main trade points are represented by the cities of Moscow and Vladivostok (as terminal points), Ekaterinburg and Irkutsk (as intermediary points) and St. Petersburg as the focal point for entering the European market, due to the proximity of the city to the European borders, the excellent transportation system and the presence of several ports linked with Western Europe[178]. Another sector of the illegitimate economy which sees a deep involvement of the *Rossijskaja Organizacija* is represented by the illegal trafficking of firearms, whose routes originates in Russia itself, due to the large quantities of firearms of the Soviet period available, which are trafficked to other regions and towards Europe mainly through the Balkans[179]. As far as other activities are concerned, the *Rossijskaja Organizacija* is involved migrant smuggling, from Siberia and the Russian Far East and then smuggled through Russia and Europe and human trafficking for sexual exploitation, in particular of women, which are smuggled throughout the Russian Federation and the former Soviet Republics, to be then destined to the European illegal sex-industry, mainly by low-scale organised crime groups. Other fields of activity are extortion, property rights, racketing and trade of stolen cars.

5. Rossijskaja Organizacija networks

As observed by Galeotti the Russian criminal underworld is not defined by a tight hierarchical structure and a single group striving for hegemonic control over a given territory as the Italian mafia. There are rather several groups with different extensions, cooperating among them for specific criminal activities. Therefore, the structure of the *Rossijskaja Organizacija* resembles more a network with loose and flexible organisation[180]. Different networks which constitute the wider phenomenon of the *Rossijskaja Organizacija* operate within the Russian Federation and abroad, by means of the "elected" representatives of the different groups. A classification is provided by Galeotti, according to ethnicity, however, it has to be underlined that any categorisation of the phenomenon is not exhaustive due to the flexible nature of the *Rossijskaja Organizacija*,

[177] Ibidem.
[178] Ibidem.
[179] Savona Ernesto U. and Mancuso Marina (Eds.). 2017. *Fighting lllicit Firearms Trafficking Routes and Actors at European Level*. Final Report of Project FIRE, (Milano: Transcrime – Università Cattolica del Sacro Cuore, 2017). Available at: www.fireproject.eu.
[180] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven and London: Yale University Press, 2018).

including more structured organised criminal groups as well as loose networks, small criminal clusters and even single individuals. Two main categories can be mentioned, the Slavic and Caucasus groups. Among the Slavic groups the most relevant are the *Solncevskaja Bratva*, based in Moscow, the *Tambovskaja Bratva*, based in St. Petersburg and the *Uralmaš gruppirovka*, based in Ekaterinburg and active in Siberia. Then, the Caucasus groups, which are composed by loose networks of Georgian and Chechen origin.

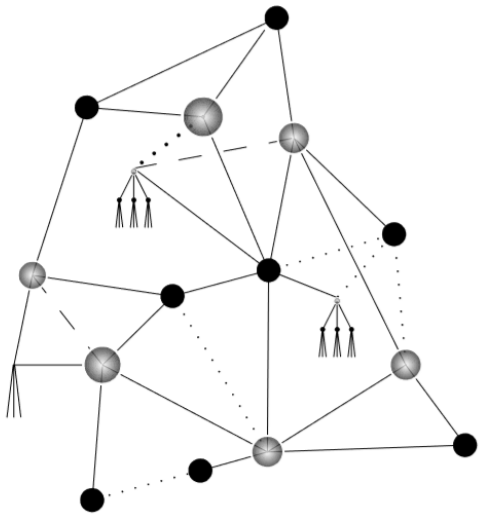
5.1. The Solncevskaja Bratva

Solncevo or *Solncevskaja* network is considered the most threatening Russian organised criminal group. It originates in the South-western district of Moscow, founded in the 1980s by Sergej Anatol'evič Michajlov**,** alias 'Mikhas', and Viktor Sergeevič Averin, alias 'Avera'. It has a strategic position within Russia, since the South-western region of Moscow is a crossroad for the airports of Vnukovo and Domodedovo and the main transportation infrastructure towards Moscow. At the beginnings, the group was considered to follow the old traditional model of the *vory v zakone* ('thieves-in-law'), however, after the fall of the Soviet Union in 1991 it turned to a more modern and flexible model. According to the classification of organised criminal groups proposed by the United Nations Office on Drugs and Crime (UNODC)[181] the contemporary *Solncevskaja Bratva* can be categorised as belonging to the 'criminal network' model. This type of organised crime group is characterised by the activities of the apical members of the network and the relevance given to personal connections rather than social or ethnic identities. Moreover, other minor groups joined the *Solncevskaja Bratva*, among which the *Orechovskaja Bratva*, headed by Sergej Timofeev and the criminal groups headed by Arnold Tamm, Aleksandr Averin and Gennady Šapovalov. According to the report of the Spanish Information Headquarters of the General Directorate of the Civil Guard[182] the *Solncevskaja Bratva* started to operate as an organised crime group in 1988, when was formed by 30 leaders, each at the head of 500-600 members. The areas of activities were quite diversified, operating in the illicit drug trafficking, illicit firearms trafficking, smuggling of goods, exploitation of prostitution and extortion. An evolution was registered with the transition from the state-run market towards a capitalistic system, when the *Solncevsakja Bratva* began to be increasingly involved into the legal economy, tightening contacts with the corrupted political establishment of post-Soviet Russia. As far as the structure is considered, the *Solncevskaja* networks considerably expanded in the 2000s, when it counted at least 2.000 active members distributed in 10-12 brigades, each composed by a number of components ranging from 15 to 40. It presents a structured organisation, with an established hierarchy responsible for the decisions and the planning of the criminal activities, however, generally the *Solncevskaja Bratva* operates within the framework of a flexible network. Nevertheless, as reported by Spanish

[181] UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, September 2002. Available at: https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf.
[182] Dirección General de la Guardia Civil – Jefatura de Información, *Informe sobre la organización criminal euroasiática SOLNTSEVSKAYA. Vínculos con los sujetos investigados. Otras relaciones criminales*, 2016. Available at: https://tbcarchives.org/tag/solntsevskaya/.

Information Headquarters of the General Directorate of the Civil Guard[183], four main levels of organisation have been detected. The first one is composed by the leaders (Michailov, Averin, Tamm, Ljustarnov, Šapovalov), whose main functions are the establishment and management of the criminal strategy, the resolution of internal and external conflicts, the distribution of the profits among the leaders, the management of the *obščak* ('common fund') and the general direction of the group. The second group is charged with the information gathering, commercial espionage, recruitment of influential personalities in the public and private sectors. The third group is tasked with planification and execution of the criminal operations. The fourth group is involved in the financial management of the network and of the criminal operations within the legal economy. Moreover, the *Solnceskaja Bratva* presents a high degree of cooperation with other groups affiliated with the *Rossijskaja Organizacija*, as well as with foreign organised crime groups such as the Italian mafia (especially with the Calabrian *'Ndrangheta* and the Neapolitan *Camorra*), the Japanese *Yakuza* and the Chinese Triads. Taking into account the extension of the network, as observed by Galeotti, the *Solncevskaja Bratva* is largely present in Russia, Ukraine (particularly in the Eastern Russophone regions of Donec'k and Luhans'k), Crimea, Lithuania, Northern Kazakhstan (where there is a wide community of ethnic Russians), as well as Israel, Europe and the United States[184]. A recent investigation in Europe has led to the arrest of one of the main leaders of the network, Arnold Arnoldovič Spivanoskij (formerly known with the last name 'Tamm') in Malaga (Spain) together with Oleg Kuznecov, Sergej Dožděv, Aleksander Grinberg and others accused of fiscal evasion, money laundering activities and involvement in criminal activities carried out by the *Solncevskaja* organised criminal group in Europe[185].

Fig.4 The 'criminal network' model



Source: UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, 2002.

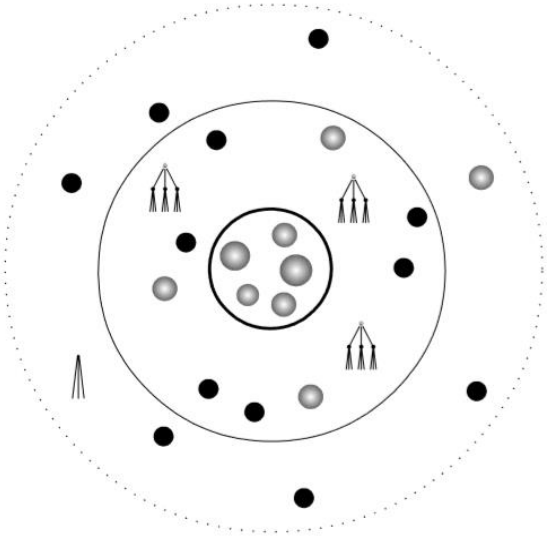
5.2. The Tambovskaja Bratva

The other major Russian organised crime group with a transnational character is represented by the *Tambov* gang also known as *Tambovskaja Bratva*. It was founded in St. Petersburg in 1988 by Valerij Ledovskich and Vladimir Kumarin, both coming from the Tambov region in the South-east of Moscow. Considering the structure, the contemporary outlook of the *Tambovskaja Bratva* can be ascribed to the model of the 'core

[183] Ibidem.
[184] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven and London: Yale University Press, 2018). pp. 146-149.
[185] Transborder Corruption Archive, Dirección General de la Guardia Civil – *Jefatura de Información, Anális parcial contenido teléfono de un investigato*, 2018. Available at: https://tbcarchives.org/tag/solntsevskaya/.

group' conceptualised by the United Nation Office on Drugs and Crime[186]. The 'core group' criminal model is characterised by a limited number of components and a relatively tight hierarchy, surrounded by an extensive loose network of temporary members participating in specific criminal activities, according to the needs of the organisation. Another characteristic of a 'core group' is the absence of a social or ethnic identity and the maintenance of a low-profile within the territory where it operates, due to the fact that the main aim is not domination over a given area, rather considerable profits for a limited number of individuals in charge of the leadership. At the beginning the *Tambovskaja* group was mainly involved in extortion and protection racket, then, by the end of the 1990s, it became involved in the legal economy, investing in a number of Russian-based companies. In particular, the Tambov organised criminal group became interested in the energy and transport sectors, acquiring control over the Petersburg Fuel Company (PTK) and of up to 100 industrial enterprises in the city of St. Petersburg[187]. Therefore, the criminal members of the network began to operate in the legitimate economy, establishing connections in the political spheres. The specialisation field was money laundering and by the 2000s the group dominated the economic sector of the city of St. Petersburg. Consequently, law enforcement authorities engaged in a systematic fight against the *Tambovskaja Bratva*, which ended with the arrest of the leader Kumarin in 2007 for money laundering and fraud[188]. The contemporary *Tombovskaja Bratva* changed nature, renouncing to the control of local territories and concentrating its activity abroad and in the management of the international illicit flows passing through Russia. As analysed by Galeotti, different criminal cells affiliated with the *Tambovskaja* organised criminal group were found in the Baltic countries, Germany and Spain, where they operate in the legal economy, investing in shell companies and managing the Russian money laundering schemes.

Fig.5 The 'core group' model



Source: UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, 2002.

5.3. The Uralmaš gruppirovka

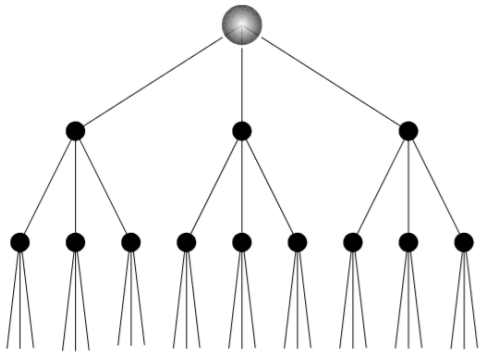
The third relevant Slavic organised crime group within the *Rossijskaja Organizacija* is represented by the *Uralmaš* group. As observed by Galeotti[189], the members of the so-called *Uralmaš* group were native of the

[186] UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, September 2002. Available at: https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf.
[187] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven and London: Yale University Press, 2018). pp. 142-145.
[188] Ibidem.
[189] Ibidem.

city of Ekaterinburg, a city in the Urals that was inhabited in the second half of the twentieth century by a considerable amount of former Gulag convicts (also known as 'blue gangs' for their tattoos), which laid the basis of the criminal underworld in the community, mainly involved in racketing and extortion activities.

During the 1980s a new group of criminals emerged in the Ordzhonikidze neighbourhood, also known as *Uralmaš,* from the name of a vast industrial conglomerate, the *Ural'skij Mašinostroitel'nyj Zavod*. This group merged in the 1990s around the leading figures of the brothers Gregorij and Konstantin Tsganov, which recruited a large number of disappointed and unemployed former workers in the *Ural'skij Mašinostroitel'nyj Zavod* also known as *Uralmaš,* from which the group derived the name. By 1993 the *Uralmaš gruppirovka* acquired the hegemony over the city of Ekaterinburg, after a bloody and cruel confrontation with the former organised crime groups operating in the area. The main aim pursued by the *Uralmaš* group was the penetration in the legal businesses, taking control over the territorial companies and the political legitimacy, obtained through participation in the local politics. Considering the structure, it can be ascribed to the 'standard hierarchy' model according to the UNODC[190] categorisation, characterised by the presence of a single leader, a tight hierarchy, a defined system of internal discipline and strong social and ethnic identities. Moreover, another specific feature of the criminal groups belonging to the 'standard hierarchy' model is their high visibility, in fact usually these groups are widely known in the area were they operate with a specific name and for their indiscriminate use of violence, through which they establish a hegemonic control over the target territory. In the 2000s, after the ascension to power of Vladimir Putin and the iron fist exercised by the government against organised criminal groups unwilling to be subordinated to the central power, the *Uralmaš* group was quite easily weakened and its main structure dismantled by the law enforcement authorities, due to the high visibility of the group and its components. The contemporary outlook of the former dominant group of the city of Ekaterinburg resembles nowadays that one of a restricted cluster of powerful criminals operating in the legal economy and coordinating their activities maintaining a low profile within the society[191].

Fig.6 The 'standard hierarchy' model



Source: UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, 2002.

[190] UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, September 2002. Available at: https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf.
[191] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven and London: Yale University Press, 2018). pp. 129-133.

5.4. The Georgian clans

The Georgian criminal underworld has a long historical tradition, in fact it is attested that even before the 1918 Russian revolution, there was a consolidated Georgian criminal structure. Nonetheless, in the aftermath of the Bolševik revolution a change was introduced, particularly in the relation of the criminal underworld with the state apparatus. Moreover, as observed by Shelley[192], the rise to the power of Stalin had as a consequence the parallel rise of the criminal groups associated with him. This ascension to a powerful position of the Georgian organised crime groups is also demonstrate by the extension of their presence in the criminal underworld, as reported by Shelley, by 1991 almost one-third of the *vory v zakone* ('thieves-in-law', in Georgian: *kanonieri qurdebi*) in the Soviet Union were Georgians, an incredible number considering that the Georgian population represented about 2% of the whole Soviet population. In the aftermath of Stalin's death, with the weakening of the state control over the economy, the Georgian criminal groups became deeply engaged in the shadow economy with the cooperation of corrupted officials and governmental figures, thus giving birth to a new crime structure based on a criminal-governmental nexus. Therefore, the new criminals which emerged in the 1970s rejected the old traditions of the *kanonieri qurdebi,* which imposed the absolute prohibition of collaboration with the government and started a new form of crime, taking advantage of the considerable underground economy shaped by the deficiencies of the Soviet system. It was only in the 1980s that the Communist Party began to considerate the Georgian criminal groups as a threat to the State and for this reason extensive anti-crime campaigns and purges were initiated that had as result the transplantation of the Georgian crime in the other Soviet Republics and most notably in Russia, thus strengthening the Georgian diaspora. One of the leading figure of the Georgian organised crime, Dzhaba Ioselani, emerged exactly in the context of the Georgian diaspora in Russia and took advantage of the 1980s reforms, being able to infiltrate Georgian politics and even of founding a nationalist paramilitary party, the so-called *Mkhedrioni* ('Knights'), mainly involved in criminal activities[193]. Ioselani and his group penetrated the political and economic spheres of the Georgian society and despite his death in 2003, still his affiliates maintain a dominant position in the city of Tbilisi, where many of the most relevant contemporary real estate investments are owned by Ioselani's associates[194]. The other major Georgian organised criminal group was that one around the leadership of Tariel Oniani, which operated mainly outside Georgia due to the anti-crime campaigns conducted in the 2000s. The Oniani's group operated extensively in Russia and also in Europe, merging with the one of the major Georgian criminal groups based in Russia, the Kutaisi clan, whose leader Merab Dzhangveladze became his main associate. Moreover, as analysed by Slade[195], the main activities in which the Georgian criminal groups based in Russia and Europe

[192] Shelley Louise, "Georgian organized crime" in Shelley Louise, Scott Erik R. and Latta Anthony (Ed.), *Organized Crime and Corruption in Georgia,* (London and New York: Routledge, 2007). pp. 61-68.
[193] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven and London: Yale University Press, 2018). pp. 166-180.
[194] Shelley Louise, "Georgian organized crime" in Shelley Louise, Scott Erik R. and Latta Anthony (Ed.), *Organized Crime and Corruption in Georgia,* (London and New York: Routledge, 2007). pp. 55-60.
[195] Slade Gavin, *Mafia and Anti-Mafia in the Republic of Georgia: Criminal Resilience and Adaptation Since the Collapse of Communism*, (Oxford: St. Antony's College, 2011).

are involved result to be illegal drug trafficking, extortion, debt collection, gambling and car theft. The structure of both Iosealani and Oniani's organisations can be ascribed to a 'standard hierarchy' model according to the UNODC classification[196] of organised crime groups. In fact, both groups present a structured and tight hierarchy built around a single leader, a high level of discipline and centralisation and single ethnicity of the members. Another Georgian group, that shows a different structure is the so-called *Tbilisi* clan, whose leader Aslan Usoyan was murdered in 2013. The Usoyan's group is structured as a 'criminal network' made up of loose affiliation, lack of a strict hierarchical order and characterised by the multi-ethnic nature of its components. Moreover, another element of divergence of the *Tbilisi* clan with the Iosealni and Oniani groups is the geographical extension of the criminal activities. The *Tbilisi* clan deploys operations mainly in Russia, particularly in the Northern and Eastern district of Moscow, while outside the Russian Federation it is active in Ukraine, Moldova, Belarus, Armenia and Georgia. However, only sporadic activities were carried out in Europe (mainly in Spain, Greece and the Balkans) and North America[197]. By contrast, both the Ioselani and Oniani groups have extensive connections with European organised crime groups and carry out operations in Western European countries.

Furthermore, considering on the one hand Georgian organised crime and Slavic crime groups on the other, a number of differences emerge. For instance, Slavic groups are not grounded on familial or clan ties, while the Georgian organised crime groups consider them as fundamental for the belonging to the clan. Moreover, Georgian organised crime groups are based on kinship networks and belonging to the same region, this holds true also for the majority of the Georgian clans based outside the country of origin. In this perspective the Georgian organised crime is similar to the mafia phenomenon, particularly to the Italian mafia, to whom familial ties and common origin are distinctive features.

5.5. The Čečenskaja bratva

Another group native of the Caucasus region is the *Čečnskaja bratva*, which registered an increase in its presence in the Russian Federation and Europe during the 1990s. The Chechen groups belong to the so-called *gorets* ('highlander', 'mountaineer'), like the Georgian crime groups, with which they share a common culture and also the organisational nature based on kinship, familial ties, loyalty and ruthless violence. However, the Chechen groups are not considered to be affiliated with the tradition of the *vory v zakone* as the Georgian ones and generally they are presented as detached from the Russian criminal underworld. Their structure is not hierarchical, rather it resembles to a loose network but culturally cohesive and with a strong nationalistic character, as pointed out by Galeotti[198]. Moreover, the main groups operating in Russia and from there handling illicit trafficking towards Europe are the Chechen groups around a criminal known as 'Malik' and

[196] UNODC, *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, September 2002. Available at: https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf.
[197] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven and London: Yale University Press, 2018). pp.173-177.
[198] Ibidem. pp. 159-163.

affiliated with the *Ostankinskaja* network, based in the North-eastern districts of Moscow, active until the 2000s; a second large group is represented by the *Lazanskaja*/*Centralnaja* clan, under the leadership of Movladi Altangrijev (alias 'Ruslan') and Chož -Achmed Nuchajev, mainly involved in racketing and extortion; a third group is that one under the leadership Nikolaj Suleimanov known as *Južnoportovaja* clan, operating mainly in the financial system; while, a fourth relevant group is represented by the *Avtomobilnaja* gang[199]. The *Čečnskaja bratva* has been increasingly overwhelmed by the Slavic groups in Russia, which imposed control over the major Russian cities. On the other hand, Chechen groups result to be active in Europe, also due to the increase of Chechen migrants in the 2000s, when European countries released the refugee status to Chechens escaping from war. The threat is particularly relevant in the case of Germany, where the Chechen groups are active in the Northern and Eastern regions of the country, mainly involved in illicit drug trafficking, theft and extortion. Furthermore, it is estimated that one of the largest Chechen diaspora community is based in Germany, even if specific data about the number of Chechens living in Germany are not available, as observed by the Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge –Bamf), due to the fact that the Chechens are registered as Russian nationals. However, the Bamf estimates the number of North Caucasians in Germany at up to 50.000, about 80% of which are Chechens[200]. Moreover, according to the data analysed by the Federal Criminal Police Office (Bundeskriminalamt –BKA) in 2019[201], there have been an escalation of the operations deployed by the North Caucasian organised crime groups. Their actions, as reported by the BKA, are characterised by a high level of violence and a cohesive structural organisation based on clannish values. Moreover, new trends have been observed in the Chechen groups operating in Germany, which are now involved also in collecting information about law enforcement authorities and have established contacts with Islamist radicalised groups.

6. Money laundering: the main activity of the *Rossijskaja Organizacija* in Europe

The Financial Action Task Force on Money Laundering (FATF), a policy-making body established in 1989 by the G7 Summit in Paris to promote and implement measures for combating money laundering at the international level, defines the phenomenon as the processing of the "[…] criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source"[202]. Therefore, the main goal of money laundering is to hide the sources of profits generated by illegal activities and move them without been noticed by the competent authorities.

[199] Ibidem.
[200] Bundesamt für Migration und Flüchtlinge – Bamf, *Statiskitken*. Available at: http://www.bamf.de/DE/Infothek/Statistiken/statistiken-node.html.
[201] Lehberger Roman, *BKA warnt vor Tschetschenen-Mafia*, Der Spiegel, 09.05.2019. Available in German at: https://www.spiegel.de/panorama/justiz/bka-warnt-vor-tschetschenen-mafia-a-1266338.html.
[202]Financial Action Task Force on Money Laundering (FATF), *What is Money Laundering?* Available at: https://www.fatf-gafi.org/faq/moneylaundering/.

Money laundering is one of the main activities in which the *Rossijskaja Organiacija* is involved in Europe for a number of reasons, among which the fact that Europe is considered by Russian criminals a safe haven, due to the high standards of privacy and accountability guaranteed by European banks. Moreover, money laundering activities allow us to highlight one of the main features of the *Rossijskaja Organizacija*, namely the relation with the political establishment, the so-called "criminal-governmental nexus". As stated before in the present research, during the 2000s, with the advent to power of Vladimir Putin, a new kind of relation was established between the Kremlin and the criminal underworld. A relationship based on the obedience of the *Rossijskaja Organizacija* to the Kremlin, to fulfil the so-called "vertical system". Putin has the merit to have placed order in the chaotic and anarchic nature of organised crime in Russia, that no longer has a decisional autonomy but is subjected to the state power, as a tool in the hands of the Kremlin. In this new framework, organised crime has been confined to specific areas of interest and operation, while being forbidden to engage in strategic economic sectors of the Russian Federation such as the oil, gas and defence domains. This is clearly highlighted by the case of the *Tambovskaja* group based in St. Petersburg, whose leader, Vladimir Barsukov, tried to infiltrate in the oil sector in St. Petersburg and was then arrested and accused of extortion in 2012[203]. Another example of the restructuring of the power relations between the Kremlin and the criminal underworld is represented by the case of Jurij Lužkov, mayor of the city of Moscow from 1992 until 2010. As observed by Kegö and Georgieff, Lužkov was controlling and keeping order in Moscow through an alliance with the criminal underworld, nevertheless, the fall from power of the former mayor of the Russian capital was not caused by the criminal connections, rather by the fact that Lužkov' interests were seen as threatening the Kremlin's economic interests. As a result, he was accused in 2010 of corruption and criminal connections and subsequently removed from office. The Lužkov's case points out both the "criminal-governmental nexus" and the new kind of relationship established by Putin with the criminal underworld, that one based on the subordination of the latter to the state power. The new power balance imposed since the 2000s by president Putin, had also consequences on the size of organised crime in Europe. In fact, due to the strong power exercised by the Kremlin over the *Rossijskaja Organizacija*, a number of criminals were pushed to move their money abroad, particularly in Europe and Israel, due to the unpredictability of Putin's behaviour and the volatility of the Russian market. Kegö and Georgieff[204] analyse the reasons why the *Rossijskaja Organizacija* increasingly moved its money abroad. Firstly, the political grip exercised by the Kremlin, collecting information on criminals and their resources and potentially being able to confiscate them. Therefore, moving the money abroad makes the criminal assets more difficult to be seized. Secondly, it is easier to hide the money trails if they are layered to more countries. Moreover, investigations led by law enforcement authorities are made more difficult since they require a high degree of cooperation, which is guaranteed only among countries of the European Union and less likely by non-EU countries. Two main methods are employed to launder

[203] Kegö Walter, Georgieff Alexander, *The Threat of Russian Criminal Money: Reassessing EU Anti-Money Laundering Policy*, (Stockholm: Institute for Security and Development Policy, 2013).
[204] Ibidem.

money, the first involve the purchase of property (such as real estate), since it is difficult for the law enforcement authorities to track the flows of money due to the fact that there are weaker regulations on non-financial institutions. A second way is that one consisting in the transfer of money abroad in non-EU countries, before moving them to EU countries, where the money "washed" are accepted by the Western banks. The reason behind the choice to move the money in non-EU countries resides in the fact that outside the EU there are weaker judiciary and banking systems, which are exploited as preferential channels to launder the criminal money.

6.1. The "Russian Laundromat"

An example that shows how the Russian money laundering machine works is offered by the so-called "Russian laundromat" or "Moldovan scheme". In 2014 the Organised Crime and Corruption Reporting Project (OCCRP) investigated on a money laundering case of transnational nature, perpetrated through Moldinconbank in Moldova, which allowed criminals and corrupted politicians to move, in the time span ranging from 2010 to 2014, US$ 20 billion from Russian banks to Moldincobank, where the money were first "washed" through the corrupted judicial system in Moldova and then sent to Latvia and other countries. As reported by the OCCRP, the perpetrators of the "Russian Laundromat" included businessmen with strong and even parental ties with the president Putin and the state security services[205]. As far as the volume of the illicit money laundering is concerned, it is believed to be much higher, as pointed out by Kirschenbaum and Tofilat, which sustain that the total amount of Russian money flows accounted to approximately US$ 75 billion[206]. The method employed was based on the use of shell companies to hide the sources of money, backed by the Moldovan courts signing off the transactions to legitimate them. The general pattern worked as follows: a transaction was opened between two companies, often based in the United Kingdom, which signed a bogus contract, in which company A agreed to lend company B a given amount of money (usually ranging from US$ 100-800 million). In reality, no exchange of money took place since both companies had the same owner, but the ownership was disguised by other fake owners. Usually, the bogus contract involved the participation of Russian companies, run by Moldovan citizens, which acted as guarantors of the debt. The next phase involved the refusal of the borrowing company (B) to pay back the debt granted by the loaning company (A), thus opening the access to the Russian company that guaranteed the debt. In the next step, the loaning company (A) would have brought the issue to Moldovan courts, where a judge would have compelled the Russian company to pay the debt it has guaranteed in the transaction between company A and B. Then, the Russian

[205] Organised Crime and Corruption Reporting Project (OCCRP), *The Russian Laundromat*, 22nd August 2014. Available at: https://www.reportingproject.net/therussianlaundromat/russian-laundromat.php.
[206] Kirschenbaum Joshua, Tofilat Sergiu, *Massive Russian Financial Flows Through Moldova Show Small Jurisdiction Matter*, The German Marshall Fund of the United States, 26th July 2019. Available at: www.gmfus.org/sites/default/files/Massive%20Russian%20Financial%20Flows%20Through%20Moldova%20Show%20Small%20Jurisdictions%20Matter.pdf.

companies transferred the illegal money to an account of the loaning company, which was the Latvian-based Trasta Komercbanka, by means of the Moldinconbank, an intermediary bank based in Moldova. Once in Latvia, the illegal money entered the European Union's financial system, due to the fact that this money resulted backed by a court order and clean, thus accepted by the Western banks.

6.2. The "Magnitskij affair"

Another relevant case, that underlines both the "criminal-governmental nexus" and the Russian money laundering machine is represented by the so-called "Magnitskij affair", that takes its name from the main victim of the case, Sergej Magnitskij, who died in 2009 in the Butyrka prison (Moscow), after being arrested in 2008 and accused of collusion with the Hermitage Capital Management (HCM) fund and its owner, Bill Browder, a British businessman. As reported by Galeotti[207], the HCM was established in 1996 and until 2006 was a successful foreign fund operating in the investment sector in Russia, with hundreds of millions of dollars as revenue. As a consequence, Browder and the business model of the HCM began to be perceived as a threat by the Russian establishment and competitors, thus the Russian Federation banned Browder to enter the

Fig.7 The cleaning cycle

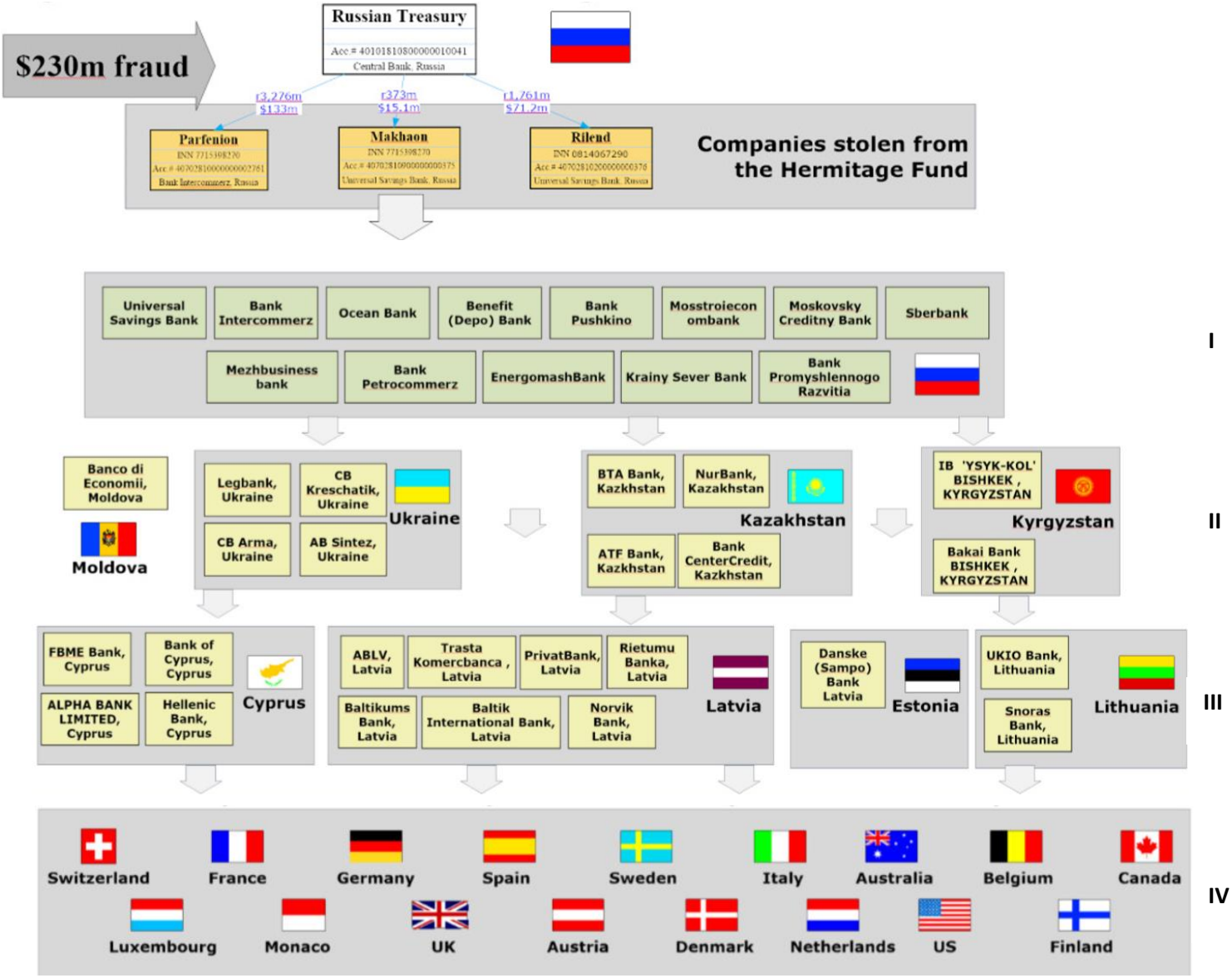
Source: Organised Crime and Corruption Reporting Project (OCCRP), *The Russian Laundromat*, 2014.

[207] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Haven, London: Yale University Press, 2018). pp.215-217.

country in 2006. The next year, a raid was organised by the police in the office of the HCM, in which computers and all relevant documents of the company were seized and subsequently used to produce false evidences of fraud perpetrated by the HCM. Then, the HCM was requested a tax refund of ₽5.4 billion roubles (US$ 230 million), to be allocated to three shell companies, from which the money would have been later transferred to the beneficiaries of the crime operation. During the public hearing of the Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (TAX3) of 29th January 2019[208], Bill Browder, CEO of the HCM exposed the result of nine years of investigation on the "Magnitskij affair", which highlights the sophisticated Russian money laundering machine. The US$ 230 million that the HCM paid to the Russian government were stolen and the person in the Russian government who authorized part of the fraudulent tax refund was Olga Stepanova, a tax official. It was later discovered that part of the money (US$11.7 million) were sent to her husband, Vladlen Stepanov, in Credit Swiss bank accounts. Then, in 2012 it was found that US$ 50 million of the US$230 billion where sent from Russia to Moldova and from there to Cyprus, Estonia, Latvia and Lithuania. The investigation conducted by Bill Browder has revealed one of the most sophisticated money laundering schemes worldwide. This scheme, the so-called "Russian Laundromat" can be summarised in four layers. The first layer is composed by Russian banks; the second layer by banks based in Moldova, Ukraine, Kazakhstan and Kyrgyzstan; then, in the third layer, there are four European Union countries with weak money laundering enforcement, namely Cyprus, Estonia, Latvia and Lithuania; while, the fourth and final layer is composed by the destination countries in Europe, US and Canada. In the investigation conducted by Browder were also identified the individuals which benefitted from the crime committed as follows: US$ 800.000 went to Sergej Rodulgin, believed to be a trustee for Vladimir Putin; US$ 2.1 million to Denis Kacyv, son of Pëtr Kacyv the former Vice-Governor of the Moscow region; US$ 11.7 million to Vladlen Stepanov, husband of Olga Stepanova, the tax officer of the Russian government that approved the fraudulent refund; US$ 294.000 to Tatiana Liksutov, wife of Maxim Liksutov, Deputy Mayor of Moscow. However, as stated by Browder, the aforementioned list is not exhaustive and more names have to be disclosed. Browder also noted that the money was employed mainly to purchase luxury goods and real estate. However, there are evidences of the fact that part of this money was fuelled to covert operations of the Russian government to support the war in Syria. In particular, it has been detected that part of the money were transferred to a bank account in Cyprus owned by a man named Isa Al Zayed, that results to be registered in the US Office of Foreign Assets Control (OFAC) sanctions list for supporting the employment of chemical weapons by the Assad regime.

[208] Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (TAX3), *Public Hearing: "Money Laundering Cases Involving Russian Individuals and their effect on the EU"*, 29th January 2019. Transcription (verbatim) available at: http://www.europarl.europa.eu/cmsdata/161080/CRE_TAX3_20190129.pdf.

Fig. 8 The money laundering scheme



Source: European Parliament Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (TAX3).

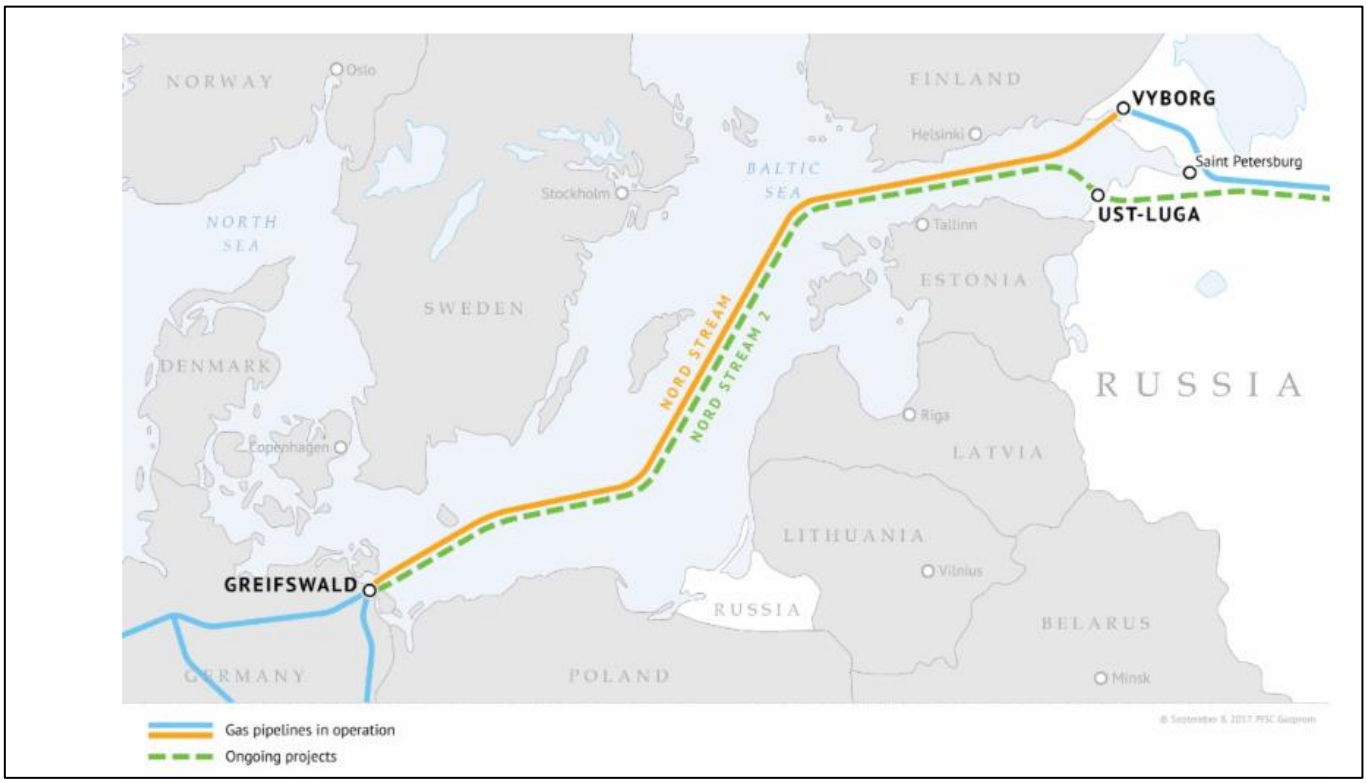
6.3. The Nord Stream Case

Another case underlining the flows of Russian black money in the EU is represented by the construction of the Nord Stream (*Severny potok* in Russian), a pipeline in the Baltic Sea inaugurated in 2011 and transporting gas from the Russian city of Vyborg to the German city of Greifswald. The project was implemented by a joint Russian-German venture called Nord Stream AG, whose main shareholder is Gazprom[209]. The project results also to be implemented by adding two other lines (Nord Stream 2), which will double the capacity of

[209] Gazprom, *Gas Pipeline: Nord Stream. The gas pipeline directly connecting Russia and Europe*. Available at: https://www.gazprom.com/projects/nord-stream/.

the pipeline to 110 billion cubic meters by 2019[210]. There are some aspects which raised doubts about how the project has been handled, the managers which were involved and the estimated cost for the realisation. As pointed out by Pasko[211], nobody knows the exact cost of the Nord Stream, since the Western parties involved provided their project budget, while the Russian parties were not transparent about the estimated costs. The official figure declared by Gazprom was of US$ 7.4 billion, but independent experts have underlined the fact that Gazprom overpriced the real cost of the gas pipelines of three or even four times. There are evidences suggesting that the official figures provided are not plausible, in fact a comparison of the cost of one kilometre of the Altai gas pipeline from West Siberia to China was declared by Gazprom to be around US$1.4 million, while calculating the cost of one kilometre of the Nord Stream it resulted to be approximately four times more. Therefore, the extra money at disposal for the project could have been employed to pay the cost of corruption components such as bribes, cuts and lobbying. Moreover, other doubts were raised in relations to the managers and board members involved in the project. It was particularly discussed, on the Western party side, the involvement of Gerhard Schroeder as the head of the joint Russian-German venture Nord Stream AG, at the time, serving as German Chancellor and close friend of Vladimir Putin, to whom Gazprom would have allegedly promised a salary of around €1.5 million per year. Another individual considered to have good relations with the Russian president was the Managing Director of the Nord Stream AG company, Mathias

Fig. 9 The Nord Stream gas pipeline



Source: Gazprom, *Gas Pipeline: Nord Stream. The gas pipeline directly connecting Russia and Europe*, 2011.

[210] Gazprom, *Gas Pipeline: Nord Stream 2. A new export gas pipeline running from Russia to Europe across the Baltic Sea*. Available at: https://www.gazprom.com/projects/nord-stream2/.
[211] Pasko Grigory, "Nontransparent and dubious actions during the construction of the Nord Stream gas pipeline" in *Russian "Black Money" in the EU: Indicators of Transborder Corruption*, EU-Russia Civil Society Forum, December 2015.

Warning, former officer of the State Security Service ('Stasi') of the German Democratic Republic (GDR)[212]. Another European official, whose involvement in the project was contested, was the former Swedish Prime Minister and Minister of Foreign Affairs Karl Bidt, accused of having private interests and returns in the project, being part of the board members of Vostok Nafta, an investment company dealing with oil and gas products from the former Soviet Union countries. Similar doubts have also been raised in relation to the construction of the Nord Stream 2, that is seen as a security threat for Europe and in particular Germany, that would be exposed to the Kremlin influence and the potential exportation of the *Rossijskaja Organizacija* in Europe through the energy sector[213]. Notwithstanding the supervisory control implemented by the European counterparts, there is always a risk in a project realised in cooperation with Russian counterparts, due to the weaker system of supervision applied and the flawed relation between the state apparatus, the business sector and the criminal underworld in the Russian Federation.

7. The presence of the *Rossijskaja Organizacija* in the European countries

The *Rossijskaja Organizacija* is involved in different activities depending on the country in which it operates. As analysed by Kegö and Molcean[214], in Austria, Cyprus, Estonia, Germany, Great Britain, Italy, Latvia, Lithuania and Switzerland the *Rossijskaja Organizacija* is mainly involved in financial crimes; while smuggling activities are concentrated mainly in the Netherlands and the Balkan region. In the following sections an analysis of the infiltration in Germany, Italy and the Baltic countries will be provided.

7.1. Case study: Germany

A large community of Russian speaking immigrants settled in Germany in the aftermath of the fall of the Soviet Union, including Russians, Ukrainians, Caucasians, ethnic Germans and Russian-speaking Jews. Moreover, even before the collapse of the Soviet Union, a considerable amount of Russians were present in Eastern Germany, due to the Soviet occupation in the post-world war II period and due to the significant amount of the so-called *Aussiedler* or Ethnic Germans from East and Southeast Europe, which were entitled to obtain the German citizenship and migrated toward Germany (Art. 116 of the Grundgesetz, Aussiedleraufnahmegesetz of 1990 and the Spataussiedlergesetz of 1992)[215]. The extension of the migration

[212] The Swiss Federal Office of Police – Service for Analysis and Prevention, *Strategic Analysis Report: Organised Crime and the Special Services of the Commonwealth of Independent States*, June 2007. Available at: https://tbcarchives.org/fsb-and-organized-crime-connection-analytical-report/.
[213] Grigas Agnia, Trakimavičius Lukas, *Nord Stream 2 is a Bad Deal for Europe*, Atlantic Council, 10th July 2018. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/nord-stream-2-is-a-bad-deal-for-europe.
[214] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 29-56.
[215] Pfetsch Barbara, *"In Russia we were Germans, and now we are Russians." Dilemmas of Identity Formation and Communication among German-Russian Aussiedler*, (Berlin: Science Center Berlin for Social Research, 1999). pp.11-12.

waves of Russians during the second half of the twentieth century towards Germany had also an impact on the implantation of Russian organised crime groups, whose main centres of activity are Berlin and Cologne. As reported by the analysis of the Bundeskriminalamt[216], a fundamental component of the *Rossijskaja Organizacija* in Germany is composed by the *vory v zakone* ('thieves-in-law'), whose ideology permeates the main groups that emerged from the gangs of post-Soviet Russia during the 1990s. A central element which has been observed is the maintenance of the old traditions of the *vory v zakone* such as the *obščak* ('common fund'), to which all the members of the criminal community had to pay a contribution, as well as a tight hierarchical structure, which is uncommon for the contemporary *Rossijskaja Organizacija*. In 2017, 29 cases were prosecuted against groups that could be assigned to the *Rossijskaja Organizacija* (5.1% of all procedures on organised crime), thus registering a decrease of 17.1% if compared with 2016 (35 prosecutions). Moreover, another aspect that has been underlined is the transnational nature of the phenomenon, since in 25 cases out of 29 the suspects acted internationally, while in the remaining four cases, only within Germany. Another relevant factor is the multiethnicity of the organised group operating under the label of *Rossijskaja Organizacija*, including individuals coming from: Armenia, Azerbaijan, Belarus, Estonia, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russian Federation, Tajikistan, Turkmenistan, Ukraine, Uzbekistan. Considering the 29 cases prosecuted in 2017, nine were dominated by Russian nationals, seven by German nationals and four by Lithuanian nationals. Particularly noteworthy is also the decline in the Georgian-dominated organised criminal groups (2017:2, 2016:5, 2015:10)[217], which can be considered as a success of the intensification of the fight against organised crime. Furthermore, almost three quarters of the whole 1.164 registered suspects possessed the Lithuanian citizenship (865 suspects), while the second most represented ethnicity was German (107 suspects) and only the third Russian (61 suspects). These data are interesting, since they show us the diversified

Fig. 10

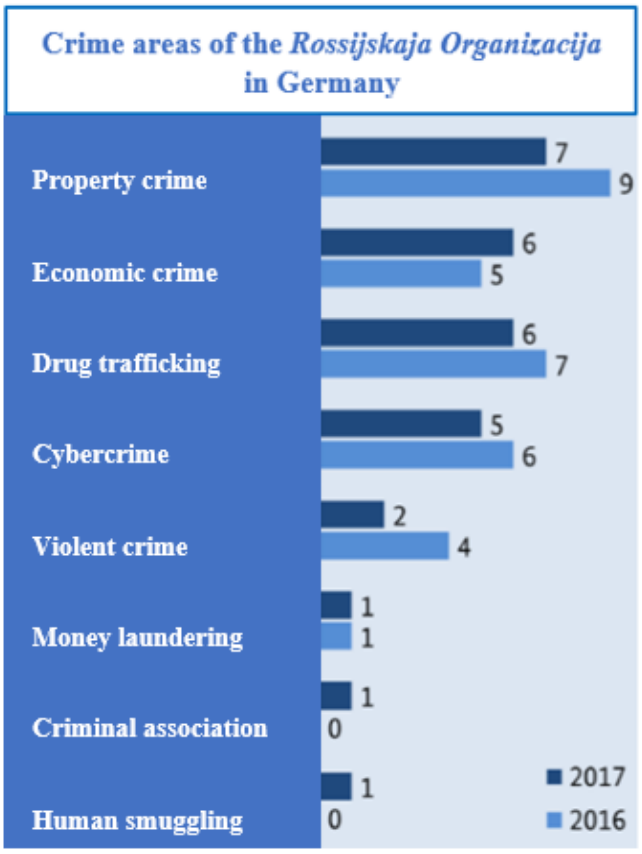
Source: Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 2018.

[216] Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 1st August 2018. Available in German at: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html.

[217] Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 1st August 2018.
Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2016*, 8th August 2017.
Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2015*, 14th October 2016.
Reports available in German at:
https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html.

nature of the *Rossijskaja Organizacija* on the one hand, and the connection with the autochthone criminal underworld in Germany. As far as the areas of activity are concerned, the criminal groups operated mainly in the property crime, drug trafficking, smuggling, financial crime and cybercrime. Particularly relevant is also the share of violent crimes (e.g. robberies) committed by the *Rossijskaja Organizacija* (15.2%) in the whole figure of those category of crimes committed in 2017 in Germany, that equals approximately a damage of €75.000 euros. However, the main sector of specialisation of the *Rossijskaja Organizacija* is the cybercrime, where it holds the largest share of crimes committed (52.9% of which 29.4% by criminals of Russian ethnicity and 23.5% by criminals of Ukrainian ethnicity) over the whole figure. The main activities carried out by the *Rossijskaja Organizacija* in the context of cybercrime are digital blackmail (29.4%) and attacks on online banking (23.5%). Other crimes committed consisted of distribution of malicious software through automated servers and botnets. Moreover, it has to be mentioned the high level of specialisation of the *Rossijskaja Organizacija* in the cyber domain and the threat posed by the use of cryptocurrencies (e.g. Bitcoin), based on a decentralised and weak regulated self-controlling system, employed as a facilitator for payment transaction in the trafficking of illicit goods via Internet underground markets (e.g. Darknet) and anonymous payment in extortion cases for money laundering activities. Among the different ethnicities included in the *Rossijskaja Organizacija*, the most represented in Germany are organised criminal groups of Russian and Lithuanian ethnicities. In 2017 have been registered 19 groups dominated by Russian criminals active in Germany, an increase of + 11.8% if compared with 2016. Considering the characteristics of these groups, usually they present a heterogeneous and not highly hierarchical structure (89.5% of the cases) based on a cooperation of different criminal clusters, lasting an average of 3.9 years. Moreover, 73.7% of their activities are conducted internationally, 5.3% at the transregional level and 21.1% at the regional level. As far as the financial aspect is concerned, Russian dominated criminal groups in Germany caused a loss equals to €1.055.307 in 2017. Taking into account the Lithuanian dominated organised criminal group operating in Germany, there have been an increase in the number in 2017 of +5.6%, if compared with the previous year. A difference with the Russian dominated groups is recorded in the structural organisation, that resulted homogenous and hierarchical for 69.4% of the groups analysed, based on a slightly higher degree of cooperation of different criminal clusters, lasting an average of 4.1 years. Another striking

Fig. 11



Source: Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 2018.

difference with the Russian dominated groups is also the geographical extent of the operations conducted by the Lithuanians, whose total of operations are directed abroad. Moreover, considering the financial aspect, Lithuanian dominated groups are responsible of an economic loss around €9.728.002 in 2017. Considering the main groups within the *Rossijskaja Organizacija* operating in Germany, they are: the *Tambovskaja* group, present in Düsseldorf and active in money laundering, prostitution and extortion activities; the *Kiolnskaja* group in Cologne, involved in smuggling and illegal trafficking of drugs and weapons[218]; the *Dolgoprudenskaja* gang, specialised in extortion crimes[219]. A number of independent criminal clusters involved in diversified criminal activities have also been observed in Frankfurt and Hamburg, while specifically in Düsseldorf the *Rossijskaja Organizacija* controls the night life and prostitution markets.

7.2. Case study: Italy

Russian organised criminal groups were transplanted in Italy by the end of the 80s. Initially these groups were operating in Italy mainly in the legal economy in the North-eastern regions of the country (Emilia Romagna, Marche, Tuscany and Veneto) and in the Adriatic Coast, specifically in the real estate business. Later, they got involved in the illegal markets as well, in the drug and arms trafficking. The *Rossijskaja Organizacija*, as the other foreign organised groups operating in Italy, is mainly active in the Northern regions due to the fact that the South of the peninsula is dominated by the Italian mafia groups, to which the *Rossijskaja Organizacija* must be subordinated, while in the North they benefit of a higher degree of independence and can freely cooperate with other organised crime groups or even challenge the Italian mafias[220]. Among the most influential groups operating in Italy, we can mention the *Solncevskaja Bratva*, whose representative in Italy in the 90s was Jurij Essine ('Samosval'), the owner of shell companies employed to launder money and import illegally oil products from Russia to Italy and arrested with the operation "Checkmate" in 1997[221]. Kegö and Moclean identify another relevant criminal group acting in Italy, the *Izmajlskaja Bratva*, involved in money laundering operations in cooperation with the *Solncevskaja bratva* and dismantled with the operation "Spiderweb" in 2002, with the arrest of the criminal representatives of the two groups in Italy, namely, Kikalişvili, Mohylevyč and Luceanskij[222].

As observed by Dalla Chiesa, Scientific Director of the *Osservatorio sulla criminalità organizzata (CROSS)* research institute of the University of Milan, the *Rossijskaja Organizacija* in Italy is not interested in

[218] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 29-31.
[219] Telegraf.rs, *Ruska mafija važi za najopasniju na svetu: Vlada surovim metodama, ima 300.000 članova, a njihove veze sa državom su veoma moćne*, 9th October 2017. Available in Serbian at: https://www.telegraf.rs/zanimljivosti/svastara/2902316-ruska-mafija-vazi-za-najopasniju-na-svetu-vlada-surovim-metodama-ima-300000-clanova-a-njihove-veze-sa-drzavom-su-veoma-mocne.
[220] Savona Ernesto U. and Riccardi Michele (Eds), *Mapping the risk of Serious and Organised Crime infiltration in European Businesses – Final report of the MORE Project*, (Milano: Transcrime – Università Cattolica del Sacro Cuore, 2018). p.122.
[221] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 45-47.
[222] Ibidem.

establishing an hegemonic control over the territory, due to the strength of the Italian mafia, rather the main aim in the peninsula is to establish close contacts with the political and bureaucratic spheres, in order to gain "protection" and deploy its operations, mainly investment of capitals and money laundering[223]. As reported by De Ficchy[224], Public Prosecutor of the Italian Republic at the Court of Tivoli, the infiltration of the *Rossijskaja Organizacija* in the Italian legal economy has been ascertained since 1995 with the arrest of Monja Elson, an investigation that revealed the presence on the Italian territory of Russian organised criminal groups involved in the investment of capitals of illicit origin in the real estate sector. A further investigation, concluded in 1997 with the arrest of 19 individuals for mafia-type criminal conspiracy, revealed the presence in Italy of one of the major Slavic group belonging to the *Rossijskaja Organizacija*, namely the *Solncevskaja Bratva* operating in Italy under the leadership of Essine in the oil products trade through intermediary companies based in Italy. Other investigations conducted during the 1990s underlined the origin of the *Rossijskaja Organizacija* in Italy and their main activities, whose nature, money laundering and investments in the real estate and touristic sectors remained unchanged through the years. Moreover, as highlighted by the *Direzione Investigativa Antimafia (DIA)* – the Italian main anti-Mafia investigation body under the Department of public Security of the Ministry of Interior – in the two 2018 semi-annual reports [225], the main groups of the *Rossijskaja Organizacija* operating in Italy belong to Georgian and Ukrainian nationalities. In particular, the Georgian groups are specialised in property crime, drug trafficking and exploitation of prostitution. They differentiate themselves from the Russian branches of the *Rossijskaja Organizacija* for the organisational structure based on a tight hierarchy and paramilitary methods; while, they show similarities in the tendency to cooperate with other foreign organised crime groups or Italian criminal associations and in the respect of a criminal code and the old criminal traditions of the so-called *kanonieri qurdebi* (the Georgian 'thieves-in-law')[226]. The main Georgian groups operating in Italy belong to the *Kutaisi*, *Tiblisi* and *Rustavi* clans, active mainly in Southern Italy, specifically in the city of Bari, in the Apulian Region. However, there are other criminal cells operating in Catanzaro, Rome, Reggio Emilia and Turin. The Georgians employ specific methods and technics, in particular in the property crime, where they apply the "lockpicking technic", consisting in opening the door locks, without forced entry. A recent case which testifies the infiltration of the Georgian organised crime in Italy has been the operation "Never Peace" of the *Arma dei Carabinieri*, the Italian gendarmerie, concluded in September 2017 in Chiavasso (province of Turin), that has detected a Georgian criminal group of 22 members, involved in property crime. It resulted to be an affiliation of the *Rossijskaja Organizacija*, following

[223] Camera dei Deputati, XVII Legislatura, *Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere*, Seduta n.205, 11th May 2017. Available in Italian at: https://www.camera.it/leg17/1058?idLegislatura=17&tipologia=audiz2&sottotipologia=audizione&anno=2017&mese=05&giorno=11&idCommissione=24&numero=0205&file=indice_stenografico.

[224] De Ficchy Luigi, "La mafia russa ed il fenomeno del riciclaggio transnazionale", Incontro di studio su tema nuove mafie: le organizzazioni criminose straniere operanti in Italia, Consiglio Superiore della Magistratura, Roma, 12-14 Gennaio 2009. pp. 7-12.

[225] Direzione Investigativa Antimafia (DIA*), Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, Gennaio – Giugno 2018, Luglio – Dicembre 2018. Available in Italian at: http://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html.

[226] Mars Gerald, Altman Yochanan, *The cultural bases of soviet Georgia's second economy*, Journal of Soviet Studies Volume 35, Issue 4, 1983. pp. 546-560.

the old traditions of the *vory v zakone* ('thieves-in-law'), such as the establishment of the the *obščak* ('common fund') in accordance with a solidarity principle of mutual assistance among criminals and the periodic *šodka* ('meeting'), with the aim of resolving the conflicts among different clans, nominating the new leaders and defining the criminal strategies. The Apulian region became a focal point for the Georgian branch of the *Rossijskaja Organizacija,* due also to the presence in the region of the largest community of Georgians in Italy, exactly 3.407 out of a total of 15.778 individuals of Georgian citizenship on the Italian ground, according to the data provided by the Italian National Institute of Statistics (ISTAT) for 2019[227]. Most of them are concentrated in the city of Bari (89,4%[228]) and it is exactly in this city that is headquartered one of the apical figures of the Georgian criminality, Merab Dzhangveladze, also known with the codename 'Jango' and leader of the *Kutaisi* clan, which is responsible for property crime, extortion and money laundering[229].

The other group extensively operating in Italy is represented by the Ukrainians, active mainly in the extortion, human trafficking and sexual exploitation[230]. A new trend observed in the last years has been that one of the migrant smuggling organised by Ukrainian criminal clusters in cooperation with Georgian and Russian clans. The path followed goes from Turkey (exactly from the district of Aksaray, Instanbul), where the migrants of Iraqi or Kurd nationalities are boarded, towards the Apulian region, to deceive the main European entry-barriers. As reported by a recent investigation[231], in the last four years more than 60 Ukrainian nationals have been arrested by the Italian authorities for smuggling of migrants, mainly of Iraqi nationality. The profits of the migrant smuggling amount, according to the estimation of the investigators, to €10.000 euros per capita for each migrant for an average of 70 migrants in each journey and an average of five thousand journeys per year.

7.3. Case study: Baltic countries

Considering the presence of the *Rossijskaja Organizacija* in the Baltic countries requires a different perspective, since in Estonia, Latvia and Lithuania the phenomenon is more rooted in the territory, due to the historical past influenced by Russia as well as the large community of Russians living in the area, especially in Latvia. According to the demographic statistics[232], in 2018 the Russians were the 25.2% of the Latvian

[227] Data extracted on the basis of specific interrogations made on the statistics elaborated by ISTAT, available at: http://dati.istat.it/Index.aspx.
[228] Ibidem.
[229] L'Espresso, *Inchiesta: Così i signori dei furti venuti dall'Est la fanno sempre franca (Ultime vittime? I Salvini)*, 30th August 2018. Available in Italian at: http://espresso.repubblica.it/inchieste/2018/08/30/news/cosi-i-signori-dei-furti-est-la-fanno-franca-vittime-salvini-1.326377.
[230] Direzione Investigativa Antimafia (DIA*), Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, Gennaio – Giugno 2018. Available in Italian at: http://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html.
[231] L'Espresso, *I trafficanti di uomini che Matteo Salvini non vuole vedere vengono dalla Russia*, 12th April 2019. Available in Italian at: http://espresso.repubblica.it/plus/articoli/2019/04/11/news/i-trafficanti-di-uomini-che-salvini-non-vedescafisti-russi-1.333644.
[232]Centrālās statistikas pārvaldes datubāzes, Latvija. Available at: https://data.csb.gov.lv/pxweb/lv/iedz/iedz__iedzrakst/IRG080.px/?rxid=cd00d9dc-a4e4-4b85-a975-e8b416dee23e.

population, being the largest minority group in the country. Latvia has been deeply influenced by Russia and the origin of the relations between the two countries traces back to the eighteenth century, when the territory of nowadays Latvia was annexed by the Russian Empire in 1795 until 1917, when, in the aftermath of the Bolševik revolution, Latvia gained the independence. However, it was exactly during this first occupation that a policy of Russification was initiated, the cultural assimilation of non-Russian communities in terms of culture and language and the implantation of Russians within the territory, that has been defined by Latvian historians as a colonisation[233]. The second wave of Russification in the area occurred during the Soviet occupation in the 1940 until 1991, interrupted by the Nazi occupation of Latvia from 1941 until 1944[234]. Consequently, the number of Russians living in Latvia drastically increased under the Soviet occupation from 10.5% in the interwar period to 34% in 1989[235]. Still nowadays the Russian minority in Latvia has a relevant social and political impact on the country, that results to be divided between European and Russian values. Moreover, during the Soviet occupation, a considerable number of former prisoners was transferred in Latvia, where they perpetrated their criminal activity and maintained their connections with the criminal underworld in the Soviet Union and the Soviet Republics[236]. Therefore, an autochthone criminal community linked with Russia developed in Latvia during the Soviet occupation and this is the reason why the *Rossijskaja Organizacija* networks in Latvia are not considered as an exogenous phenomenon, rather as an indigenous one, as observed by Kegö and Molcean[237]. In fact, the presence of a large Russophone community in the country is a facilitator for the penetration of the *Rossijskaja Organizacija*, as demonstrated also by other areas where there are relevant communities of Russian expats such as in Costa del Sol in Spain and in Cyprus. Moreover, Latvia holds a relevant position in the context of the illicit traffics from Russia towards the EU, due to its geographical position and the transportation infrastructure by land, air and sea. Therefore, Russian organised crime employs Latvia as a transit country for illicit trafficking and as a stationary base for financial and economic crime, especially in the money laundering sector. As reported by Europol[238], Latvia is one of the main hubs in Europe for the illicit drug trafficking and smuggling of goods from East towards the West. In fact, as analysed by Galeotti[239], almost one third of the Afghan heroin delivered on the European market passes through Russia and reaches Europe through focal points as Riga, whose port is also a favoured mean of connection with St. Petersburg for the trafficking of illicit goods (e.g. excise goods or stolen cars) from Europe towards Russia.

[233] Strods Heinrihs, "Sovietization of Latvia 1944–1991" Nollendorfs Valters, Oberländer Erwin (Ed.), *The Hidden and Forbidden History of Latvia under Soviet and Nazi Occupations 1940-1991*, (Riga: Institute of the History of Latvia, 2005). pp. 209-227.
[234] Lumans Valdis O., *Latvia in World War II*, (New York: Fordham University Press, 2006). pp. 173-209.
[235] Wieclawski Jacek, *The Case of the Russians in Latvia and the Need of the Comprehensive Research Approach in Contemporary International Relations*, Institute of Political Science, University of Warmia and Mazury in Olsztyn, Poland, February 19, 2015.
[236] Vilks Andrejs, "Latvia" in Kegö Walter, Molcean Alexandru (Ed.), *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, (Stockholm-Nacka: Institute for Security and Development Policy, 2012). pp. 67-77.
[237] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 47-50.
[238] EUROPOL, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017. Available at: https://www.europol.europa.eu/socta/2017/.
[239] Galeotti Mark, Crimintern: *How the Kremlin uses Russia's Criminal Networks in Europe*, European Council of Foreign Relations, April 2017.

Always taking into account the illicit drug market, Latvia, alongside with Lithuania and Estonia, is also becoming a preferential site for the trafficking of cocaine coming from Latin America and in minor part from Russia[240]. Moreover, the *Rossijskaja Organizacija* is involved in money laundering activities in Latvia, as demonstrated by the so-called "Russian Laundromat", whose financial sector results to be extremely vulnerable. In fact, during the last decades, the Latvian financial system has been systematically exploited by criminal groups of the former Soviet Union to facilitate the transfer of approximately €20 billion euros of illicit money into the European and international financial system[241].

Considering Estonia, the characteristics of the *Rossijskaja Organizacija* are similar to those ones in Latvia. In fact, Estonia as well has an historical relation with Russia and a considerable community of ethnic Russians. According to the demographic statistic of 2019[242], the whole Russian ethnic group in Estonia accounts for 24.8% of the total population, resulting the largest minority group in the country. Moreover, like the other Baltic countries, Estonia experienced the domination of the Russian Empire from the eighteenth century until 1918 and then of the Soviet Union from 1944 until 1991 and was subjected to the policy of Russification that consequently resulted in the emergence of a strong and compact community of ethnic Russians, which persists nowadays and influence the political and societal layers of the Estonian state. As far as the emergence of the criminal underworld is concerned, what must be underlined is that it was shaped on the Russian criminal model. As analysed by Lill[243], the groups formed in the 1980s were generally headed by ethnic Russians and the respect of the criminal rules and old tradition of the *vory v zakone* ('thieves-in-law) was imposed. The original criminal networks were characterised by a tight hierarchy and the widespread use of ruthless violence, however, after the fall of the Soviet Union in 1991 a major change took place. In the post-Soviet period, the organised criminal groups in Estonia shifted towards a new pattern, being more and more involved in the legal economy, renouncing to violence as a specific *modus operandi* and increasingly penetrating the political and economic levels of the society. During the transition to the market economy the criminal underworld could benefit of the new opportunities opened by the capitalist system, particularly in the financial sector, where a deep-rooted money laundering mechanism linked with the Russian Federation was established. Moreover, alongside with the traditional illicit trafficking of drugs, weapons, human beings and excise goods, the Estonian crime groups affiliated with the *Rossijskaja Organizacija* have showed, in the last decade, an increasing interest in the real estate sector, as a necessary component of the wider money laundering machine, for the hiding of capitals flowing from Russia and then invested in Estonia and other European countries. Nevertheless, the main activity carried out by the branches of the *Rossijskaja Organizacija* in Estonia is linked to the illicit trafficking of drugs, mainly of heroin and amphetamines, towards Finland and other European

[240] Loskutovs Aleksejs, *Transnational Organised Crime – Latvian Challenges and Responses*, Connections QJ, No. 3, 2016.
[241] Transparency International Latvia (Sabiedriba par atklatibu – Delna), *Connections. Money laundering in Latvia and the role of trust and company service providers*, January 2018.
[242] Rahvaarv rahvuse järgi, 1. Jaanuar, aasta, 6th June 2019. Available at: https://www.stat.ee/34267.
[243] Lill Liis, "Estonia" in Kegö Walter, Molcean Alexandru (Ed.), *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, (Stockholm-Nacka: Institute for Security and Development Policy, 2012). pp. 54-66.

countries, which is handled primarily by one of the oldest criminal group in Estonia, the *Kemerovskaja bratva*, operating since the 1990s, whose main leaders have been arrested in 2017 in Spain by Estonian central criminal police[244] in a joint operation with Spanish national police[245]. In addition, a new trend that has been observed is also the high specialisation of the Estonian criminal groups linked with Russia in the cyber domain, particularly in the financial and economic sectors, were different cybercrimes are committed against public institutions, private enterprises and individuals.

Then, considering Lithuania, the pattern of the organised criminal groups affiliated to the *Rossijskaja Organizacija* is the same observed for Latvia and Estonia. In fact, Lithuania as well was subjected to the Russian domination in 1795 until 1918 and then from 1944 until 1991. Moreover, in Lithuania as well the criminal underworld developed as an appendix of the *vory v zakone* in the Soviet Union. What is peculiar of Lithuania is the fact that shares the border with the Russian exclave in Europe of Kaliningrad, from which the illicit trafficking of drugs and goods enter in Lithuania. The main activities in which Lithuanian organised criminal groups affiliated with the *Rossijskaja Organizacija* result to be involved are drug trafficking, human trafficking and labour exploitation, tobacco and alcohol smuggling, money laundering and smuggling of stolen luxury cars (mainly from Germany), which is become a field of specialisation for Lithuanian criminals [246]. As observed by Siegel[247], there are two main criminal poles in Lithuania, the first is Vilinus, where emerged the historically most important criminal groups (*Vilinusskaja Brigada* and *Centurioni*) and which presents a mixed composition of Russian and Lithuanian members; the second criminal centre is represented by Kaunas, which is strictly nationalistic in terms of ethnicity of the members, being composed only by Russians, and where emerged in the aftermath of 1991, the *Daktarai* , *Zhaliakalnis*, *Dashkinai*, *Senamiestis* and *Kauilaniai* criminal groups. The *Daktarai* criminal group is the only one of the historical criminal associations still active in Kaunas, alongside other groups like the *Agurkiniai* and the *Kamuoliniai*. As far the contemporary outlook of the Lithuanian branches of the *Rossijskaja Organizacija* is concerned, it has to be noted that the familial, hierarchical structure has been abandoned in favour of a more flexible one, based on loose networks and a more business-oriented organisation, well integrated in the legal economy.

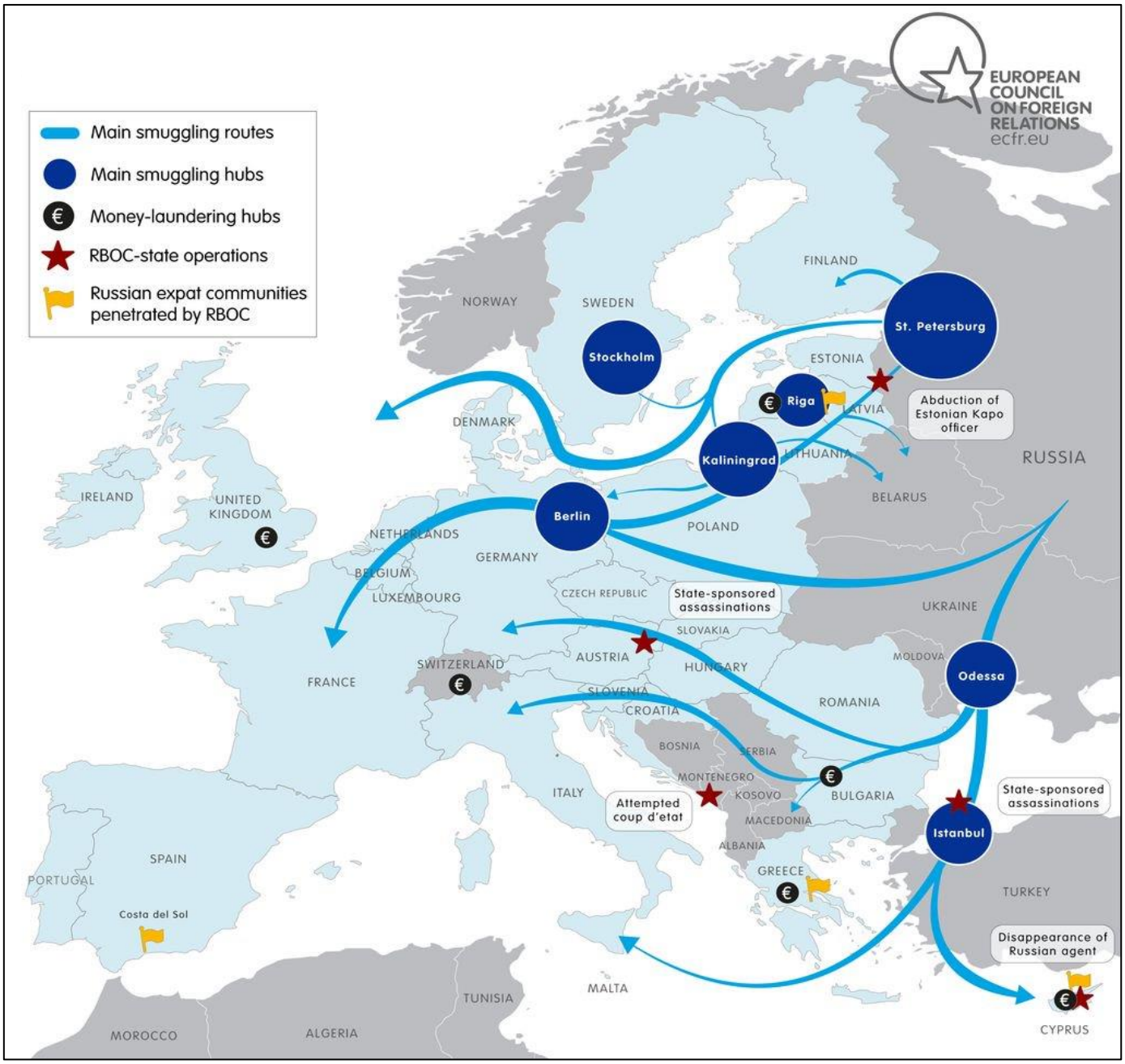
[244] Prestupnaja Rossija – Organizovannaja Prestupnost', *V Éstonii načinaetsja sud nad liderami «Kemerovskoj» OPG*, 21st January 2018. Available in Russian at: https://crimerussia.com/organizedcrime/v-estonii-nachinaetsya-sud-nad-liderami-kemerovskoy-opg/.

[245] OCCRP, *Spain: Russian Kemerovskaya Gang Leader Arrested in Joint Spanish-Estonian Operation*, 8th August 2017. Available at: https://www.occrp.org/en/component/content/article?id=6829:spain-russian-kemerovskaya-gang-leader-arrested-in-joint-spanish-estonian-operation.

[246] Gutauskas Aurelijus, "Lithuania" in Kegö Walter, Molcean Alexandru (Ed.), *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, (Stockholm-Nacka: Institute for Security and Development Policy, 2012). pp. 78-87.

[247] Siegel Dina, *Lithuanian itinerant gangs in the Netherlands*, Kriminologijos Studijos, No.2 2014.

Fig.12 The *Rossijskaja Organizacija* and its routes into Europe



Source: European Council on Foreign Relations, 2017.

IV. *ROSSIJSKAJA ORGANIZACIJA*, CYBERWARFARE AND CYBER CRIME

1. Cybersecurity: main trends and challenges

There is never enough security that can be provided to a system, a company or a country. The reason why is that security must always evolve in order to face the new emerging threats. Security needs to keep pace with the global changes and, particularly, with the rising of new technologies, which expose us to new and unknown vulnerabilities. The dynamic and rapid transformation of the cyber-space and the threats associated are valuable examples of the framework in which it is necessary to consider security issues.

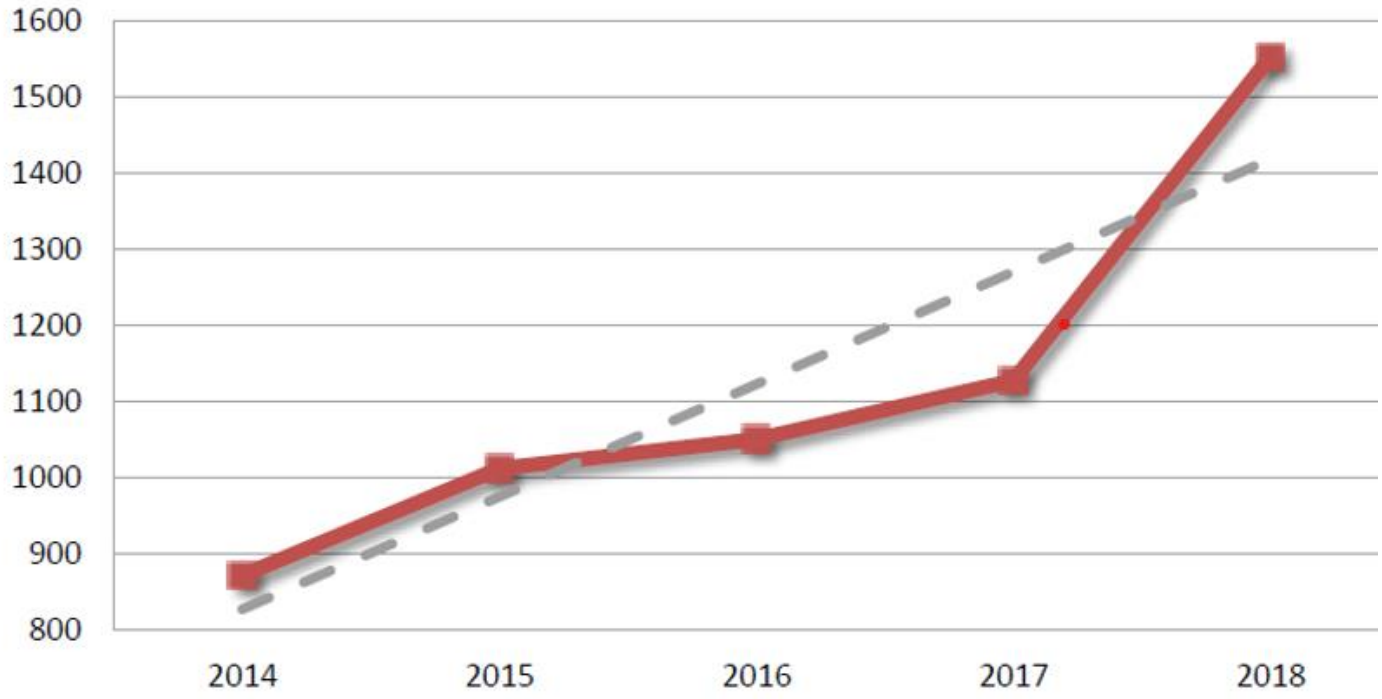
There are several definitions of security, encompassing different domains (individual, corporate, national) and aspects (military, political, economic, societal, environmental) but to understand what security truly means, we need to consider a minimal definition of the concept, that defines security as "the alleviation of threats to cherished values".[248] Security means the protection of what we care, protection of all those values and things which define us, which give us a meaning and provide us a reason to pursue our goals. It can be protection of what we care in the private sphere, or in a company or the pride and duty to defend our nation. Stated otherwise, security means to protect who we are and what we believe.

Among the different emerging threats at the global level, particular attention has been posed on cybersecurity issues, which have become a primary concern for the global security. According to the International Telecommunication Union (ITU), cybersecurity is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment."[249] Cybersecurity is an item worth investing and protecting both in a corporate an in a national perspective. In fact, according to a research conducted by CLUSIT[250] in 2018 there have been a huge increase in cyberattacks worldwide. In detail, over the last three years an increase of +77,8% of cyber-attacks has been registered, if compared to 2014 and + 37,7% if compared with 2017.

---

[248] Williams Paul D. and McDonald Matt , *Security Studies. An Introduction*, 3rd ed., (New York: Routledge, 2018), p.6.
[249] International Telecommunication Union (ITU), *Overview of cyber security, ITU-T X-Series Recommendations Data Networks, Open System Communications And Security*, Rec. ITU-T X.1205 (04/2008), p.2. (https://www.itu.int/rec/T-REC-X.1205-200804-I).
[250] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, 2019. Available at: https://clusit.it/rapporto-clusit/.

Fig.1 Number of serious cyber-attacks detected for each year (2014-2018)



Source: Clusit – Rapporto 2019 sulla Sicurezza ICT in Italia

The main categories of cyber-attacks are the following: cybercrime, cyberespionage, cyberwarfare and hacktivism. It is worth mentioning that "cybercrime" and "cyberespionage" have registered the highest number of attacks in the last eight years. In particular, in 2018 there has been an increase in cybercrime's attacks (+43,8%) and of cyber espionage's activities (+ 57,4%), if compared with data of 2017.

Fig.2 Number of cyber-attackers for category

ATTACKERS FOR TYPE	2014	2015	2016	2017	2018	2018
Cybercrime	526	684	751	857	1232	43.8%
Hacktivism	236	209	161	79	61	-22.8%
Espionage / Sabotage	69	96	88	129	203	57.4%
Cyberwarfare	42	23	50	62	56	-9.7%
Espionage / Sabotage + Cyber Warfare	111	119	138	191	259	35.6%

Source: data based on Clusit – Rapporto 2019 sulla Sicurezza ICT in Italia.

Another interesting aspect emerging from the research is the fact that nowadays is more difficult to distinguish between the two categories of attacks, those ones of "cyberespionage" and "cyberwarfare", since espionage operations are mainly directed towards states and less to companies. This aspect is relevant when analysing the activity of Russian organised crime groups within the cybersecurity domain for a number of reasons, among which the fact that according to the Russian cybersecurity doctrine, cyberwarfare is officially included into the Information Warfare (IW) and Russian-speaking cybercrime, unofficially, contributes in a fundamental way to the Information Warfare conducted by the Russian Federation to defend its national interests and pursue its goals.

The relevant aspect for the present research is to enquire the level of connivance between the Russian government and the cybercrime and how the last one contributes to the Information Warfare conducted by the Kremlin. In order to analyse this hypothetical nexus, we need to define the concepts of cyberwarfare, cybercrime and how these two categories can be included in the broader concept of Information Warfare.

2. Cyberwarfare and Cybercrime: the Russian exegesis

Cyberwarfare is defined as a conflict between states, but it can include non-state actors as well, with the aim of penetrating another nation's networks or computers, using communication technologies techniques to cause harm and disruption or steal valuable information to military, industrial or civilian targets.[251] Another concept that needs to be explained is that one of cyberspace, the dimension on which acts cyberwarfare, that is defined by Kuehl as: "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies."[252]

Then, it is necessary to consider and define cyber warfare within the Russian context, particularly, how this concept is framed into the Russian military doctrine[253]. The Russians prefer to employ the term Information Warfare (*Informacionnaja Vojna)* instead of cyber warfare. The reason behind this apparently not-relevant linguistic choice lies on the fact that *Informacionnaja Vojna* is a much broader concept than cyber warfare (*kibervojna*), including not only electronic warfare and computer network operations but also psychological operations and information and disinformation actions. What is worth mentioning is that *Informacionnaja*

[251]Arquilla John and Ronfeldt David, "Cyberwar is coming!", Vol.12 No.2 in Comparative Strategy, (Taylor & Francis: 1993). Available at https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf.
Cornish Paul, Livingstone David, Clemente Dave, Yorke Claire, *On cyber warfare*, (London: The Royal Institute of International Affairs, 2010). Available at http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf

[252] Kuehl Daniel T., "Cyberpower and National Security" in Kramer Franklin D., Starr Stuart H. and Wentz Larry K., *Cyberpower and National Security*, (Washington:National Defense University Press, 2009).

[253] Presidential Decree No.2976, *The Military Doctrine of the Russian Federation*, 25th December 2014. Available in Russian at https://rg.ru/2014/12/30/doktrina-dok.html and available in English at https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf.

Vojna is relatively new in terms of the means employed, but, as far as the reasons, the targets and the strategies employed are concerned, it is as old as the Soviet times. More generally, is one of the means at governmental disposal to dominate the information sphere for its own purposes.

Information is power, this is clear in the Russian mind, having developed a complex and in-depth strategy since Soviet times. The cyber security domain is permeated by the same Information Warfare strategy, the Russians changed only the tactics. Cyber security and information security are considered two separate things, but in the Russian military doctrine these two concepts are understood to be the same.[254] This fact has relevant consequences in the management of the information, since both technical data and cognitive data are overseen by the national security managers. The Russia's National Security Strategy 2020, clearly states that a "global information struggle" is now intensifying and the response to this threat is "truthful" information to Russian citizens, through native internet platforms and social media employment.[255] The goal for the Russians is to defend the "information space", (*inforcionnoe prostranstvo*), employing not only the broad concept of information security operations, but also computer network operations. References to this kind of operations are made several times in different official documents such as in the: Information Security Doctrine of the Russian Federation,[256] Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space,[257] and Basic Principles for State Policy of the Russian Federation in the Field of International Information Security.[258]

To explain the nexus, proposed in the present research, between the government of the Russian Federation and cybercrime, it is necessary to make a step back and analyse the concept of Information Warfare (hereinafter: IW). In the Russian political, academic and military discourse, IW is considered, on the one hand, as a set of methodologies and techniques employed to gain power and to influence the public opinion, on the other, as a tool at disposal of the West to harm Russia. In the last interpretation, IW is perceived to be a direct attack against the statehood of the Russian Federation. One of the main advocates of this exegesis is Igor Panarin, who firmly states that IW is a direct threat posed to Russia by the West, whose aim is to achieve the dissolution of the Russian Federation.[259] Three main interpretations of IW have been proposed in the Russian context: the

---

[254] Jaitner Margarita, "Russian Information Warfare: Lessons from Ukraine", chapter 10 in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications, 2015). (https://www.academia.edu/24846469/Russian_Information_Warfare_Lessons_from_Ukraine).

[255] Presidential Decree No. 537, *Russia's National Security Strategy to 2020*, 12nd May 2009. Available in Russian at http://kremlin.ru/supplement/424 and available in English at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020.

[256] Presidential Decree No. 646, *Doctrine of Information Security of the Russian Federation*, Moscow, 5th December 2016. Available in Russian at https://info.publicintelligence.net/RU-InformationSecurity-2016.pdf and in English at http://afyonluoglu.org/PublicWebFiles/strategies/Asia/Russia%202016%20Information%20Security%20Doctrine.pdf.

[257] Ministry of Defence of the Russian Federation, *Kontseptual'nye vzglyady na deyatel'nost' Voorughennykh Sil Rossijskoj Federatsii v informatsionnom prostranstve*. Available at http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle.

[258] Presidential Decree No. 1753, *Osnovy gosudarstvennoj politiki Rossijskoj Federatsii v oblasti meghdunarodnoj informatsionnoj na period do 2020*, 24th June 2013. Available at http://www.scrf.gov.ru/security/information/document114/.

[259] Panarin Igor, *Informatsionnaya Voyna I kommunikatsii*, (Moscow: Goryachaya Liniya-Telekom, 2015).

"subversion-war" (*mjateževojna*) developed by Evgenj Messner, the "net-centric war" of Aleksandr Dugin, and the "information warfare" of Igor Panarin.

According to Russian military historian and political scientist, Colonel E. Messner (1891-1974), in the twentieth century there was not a division between the military and the public domains, thus acknowledging that the population was at that time participating with different degrees of intensity to the war through public movements. He named this phenomenon "subversion-war", characterised by the fact that the army loses the monopoly over the warfare, that becomes dominated by psychological factors, propaganda and the politics. In particular Colonel E. Messner emphasised the relevance of the enemy's society, that becomes a strategic target to destroy.[260]The meaning of the struggle becomes that one of "[…] degrading the spirit of the enemy and saving your own spirit from degradation […] ".[261] The second theory, the "net-centric war", was developed by the Russian political scientist, strategist and Slavophile Aleksandr Dugin, who begins his theoretical reasoning with the assumption that Russia is neither European nor non-European, rather it belongs to Eurasia and presents a unique physiognomy, due to the fact that Russia is only partly European and mostly Asian. Exactly for this feel of belonging to the Asian paradigm, the Russians cannot fully embrace the European culture and values, because they are something else, something in-between. From this first postulate, Dugin firmly asserts that the Russian society is ontologically opposed to the Western civilisation, in particular he claims that the Russian society is permanently threatened by the West, mainly the US, throughout the 20th and 21th century.[262]According to Dugin, the Americans developed a new military strategy, the net-centric war, which includes four different domains: physical, informational, cognitive and social. He defines the "network" as an informational dimension in which strategic, diplomatic, economic and media operations are led. Dugin continues the discussion and clearly states that the Americans' primary aim is that one of exercising a hegemony over the network. This aim is pursued by achieving an absolute superiority in the informational dimension, forcing all the other populations to believe, through persuasion and flexing of muscles, that waging war against the US is useless, since any potential offender is destined to succumb.[263] For this reason, according to him, Russia must undergo to a process of post modernisation its army, secret services, political and communication institutions, in order to counter the American net-centric war and exactly for this reason the Russian Federation includes cybersecurity within the Information Warfare domain, considering cyber-attacks as a tool to defend its strategic assets and to counter the Western aggression. The third theory of Information Warfare is that one developed by Igor Panarin, asserting that there is an on-going struggle between the West and Russia, where a pivotal role is played by the informational dimension. According to the scholar, there are

[260] Messner Evgeny, "Imya Tret'yey Vseminoy" in *Vsemirnaya myatezhevoyna*, (Moscow: Kuchkovo Pole, 2004).
[261] Messner Evgeny, "Lik sovremennoy voyny", Volume 2 *of Problemy vojny i mira*, (Yuzhno-Amerikanskij otdel Instituta po issledovaniyu problem vojny i mira im. Generala prof. N.N. Golovina, 1959).
[262] Dugin Aleksandr, *Sotsiologiya geopoliticheskikh protsessov Rossii,* (Moskva: Mezhdunarodnoe «Evrazijskoe Dvighenie», 2010). Available at https://www.geopolitica.ru/sites/default/files/sgpr-1.pdf.
Dugin Aleksandr, *Geopolitika Postmoderna. Vremena novykh imperij. Ocherki geopolitiki 21 veka* (Sankt-Peterburg: Amfora, 2007). Available at https://www.klex.ru/97a.
[263] Dugin Aleksandr, *Voyna kontinentov – sovremenny mir v geopoliticheskoy sisteme koordinat*, (Moskva: Akademicheskij Proekt, 2015).

four layers in the informational-psychological confrontation, namely: political, diplomatic, economic and military and what is relevant are not the layers themselves but the manipulation of the information within these categories. Panarin draws up three phases of information warfare, the first one involves the collection of information about the enemies (strategic political analysis), the second one concerns the disinformation and manipulation of the information, while the third phase relates to all those actions to counter the Information Warfare of the adversaries (informational defence). The Information Warfare is submitted in Russia to a high level of politicisation, it is included in the broader framework of the historical offensive waged by the West against Russia. This idea is widely spread in the academic, military and political discourse, as testified by public declarations released by the Russian political leadership, among which the words of the President Vladimir Putin who asserted, during the meeting of Russian Federation ambassadors and permanent envoys in Moscow[264], the relevance of influencing and shaping the public opinion nowadays. Furthermore, the same reasoning is presented in programmatic documents such as the Russian Nation Security Strategy[265] which underlines the fact that the adversaries are increasingly relying on disinformation and falsification campaigns in order to achieve their geopolitical goals, thus highlighting the major role played by the information domain in the international affairs. An analogous reasoning is presented in the text of the Doctrine of Information Security of the Russian Federation, where it is stated that "Intelligence services of certain States are increasingly using information and psychological tools with a view to destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end. There is a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation. Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented from performing their professional duties. There is a growing information pressure on the population of Russia, primarily on the Russian youth, with the aim to erode Russian traditional spiritual and moral values."[266]What emerges from this picture is that the Russians, both the population and the political élite, perceive an on-going threat coming from abroad, whose main aim is the manipulation of information. In this context cybersecurity is valued as a high-level defence and offensive system, as a fundamental tool of the IW, that can provide protection and also allow the Russian Federation to impose itself on the global arena. As analysed by Ofer Fridman, the Russians support the restrictive decisions of the government in terms of freedom of press and control over the informational dimension exactly for the perception of the threat coming from abroad. Moreover, Fridman underlines another fundamental aspect,

[264] Speech at the Meeting of Russian Federation ambassadors and permanent envoys in Moscow, 30 June 2016. Available at http://en.kremlin.ru/events/president/news/52298.
[265] Presidential Decree No. 683, On the Russian Federation National Security Strategy, Moscow, 31 December 2015. Available in Russian at https://xn--b1aew.xn--p1ai/upload/site1/document_file/Ukaz_683-2015_d1(4).pdf and in English at http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf.
[266] Presidential Decree No. 646, Doctrine of Information Security of the Russian Federation, Moscow, 5th December 2016.

worth considering when analysing Russia, notably the Russian desire of greatness, the pride for their country and the open wound of the loss of power after the dissolution of the Soviet Union. All these elements together, at least partially, explain the degree of acceptance among the Russians of the restrictive measures adopted by the government in the informational domain, since they are emergency measures taken to defend the country. Furthermore, this perceived feeling of emergency and risk to which is exposed the national security can be analysed with a view to the nexus between the Russian government and organised crime. There are indeed evidences of the connivance between the two elements of the pair, with organised crime, in the form of cybercrime, getting more and more involved in state-driven actions to the detriment of foreign assets.

3. Cybercrime and *Rossijskaja Organizacija*

"Everyone knows that Russians are good at maths. Our software writers are the best in the world, that's why our hackers are the best in the world",[267] stated Lt. Gen. Boris Mirošnikov, MVD Department K (cybercrimes). Soviet Union always valued scientific knowledge as the highest existing science and had high expectations upon scientific progress. This belief was translated in huge efforts in terms of investment in scientific education and research, which were seen as drivers of progress and as strategic tools to assert the communist hegemony worldwide. As stated by Rifkat Bogdanov, Russian and Soviet mathematician, science reflects not only the natural world but also the needs of society. The great innovation delivered by the Soviets is that science is not considered as pure science, inaccessible to the masses, but as an organised social and economic experience in the service of society, directed towards the concerns of the working class. As observed by Alexej Kojevnikov[268], the Soviets conceptualised science both in terms of scientific materialism – science as epistemological path towards the objective truth – and within the meaning of social constructivism – considering sciences in general as subjected to a social and ideological stance. The Soviet Marxist discourse on science led to a reconsideration of the relationship between science and society, which subsequently conducted to the enormous expansion of scientific professions combined with a demographic radical change in the scientific élite, where for the first time were admitted individuals with diverse social extractions that previously were under-represented, without discrimination of gender, class origin, ethnicity or race. This fundamental turning point represents the ground on which is rooted Russian excellence in scientific knowledge, an excellence that persists up to the present day and that is clearly visible in the cyber domain.

The development of a hacking underworld in Russia is parallel to that one of the contemporary criminal community, whose rising is linked to the dissolution of the Soviet giant and the power *vacuum* thereafter. As noticed by Mark Galeotti, the Russian hacking community is the result of a combination of diverse factors, among which the well-rooted and high-level scientific training in Russia, the emergence of the first embryonic

[267] ZDNet, 6 April 2005. Speech available at https://www.cnet.com/news/russian-police-our-hackers-are-the-best/.
[268] Kojevnikov Alexei, *The Phenomenon of Soviet Science*, (Vancouver: The History of Science Society, 2008). Available at https://pdfs.semanticscholar.org/ccb5/3de6cda73022bfa0b2358899b76a3f82f8a4.pdf.

hardware on the market and the lack of adequate legal employment opportunities, all elements which led to the rise of a community of highly trained young professionals who joined the variegated Russian criminal *milieu*.[269]

3.1. Cybercrime trends and main characteristics

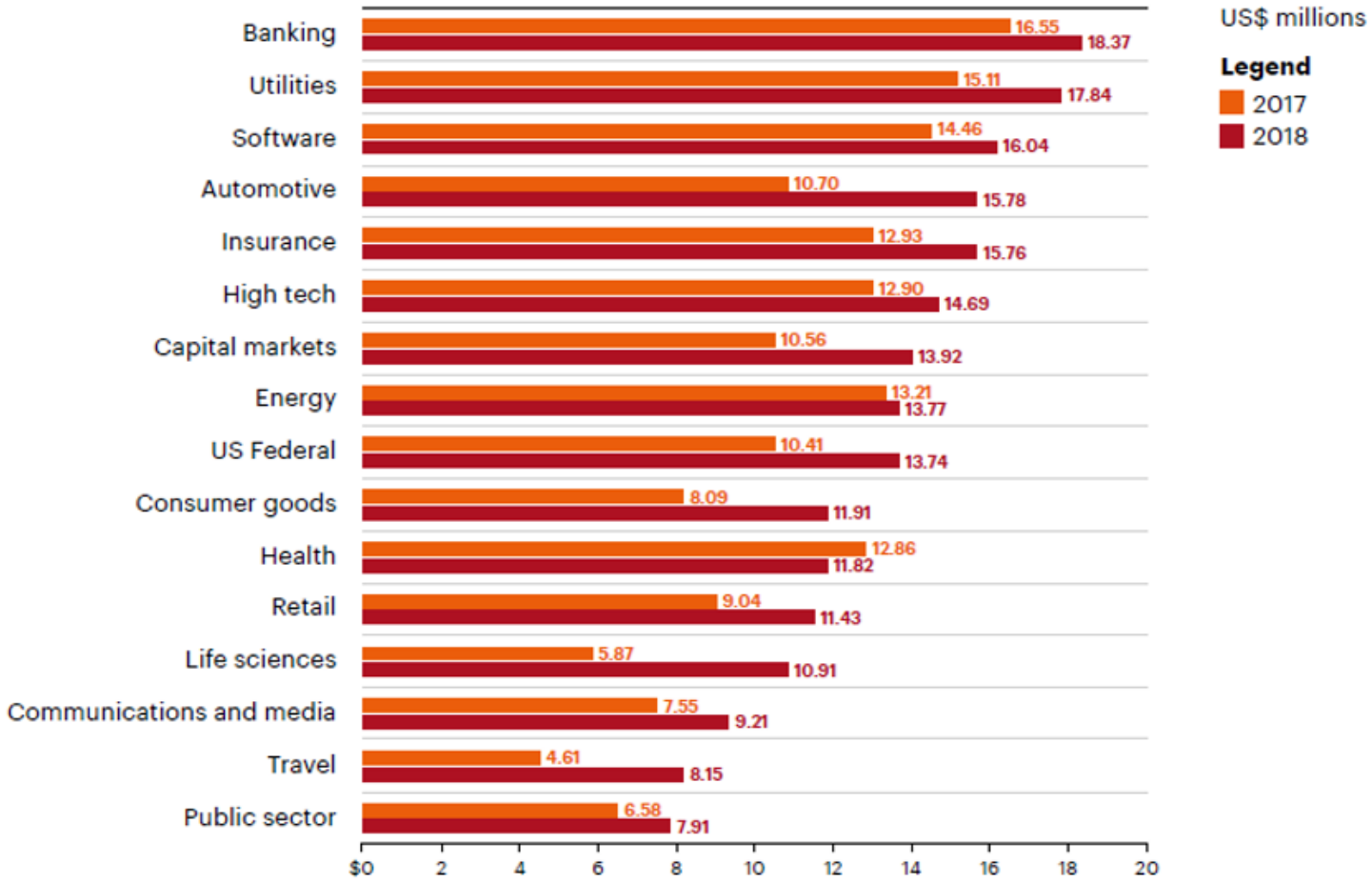
Acknowledging the lack of a unique definition of cybercrime and the fact that only few international or regional legal instruments define cybercrime, the United Nations Office on Drugs and Crime (UNODC), highlights the relevance of a description of the concept through the acts representing it, rather than a definition *per se*. According to the UNODC, there are three main categories which fall under a cybercrime offence, notably: acts against the confidentiality, integrity and availability of computer data or systems; computer-related acts for personal or financial gain or harm; computer content-related acts.[270] Cybercrime is an increasingly growing phenomenon, affecting both the private and public sectors and causing relevant damages either in terms of financial losses and reputational harm. According to the Ninth Annual Cost of Cybercrime Study released by Accenture in March 2019[271], organisations and companies have seen an increase of +11% in the number of security breaches in 2018 and an increase of +67% in the last five years. According to the aforementioned research, the total cost of cybercrime for each company increased of +12%, from US$ 11.7 million in 2017 to US$13.0 million in 2018. The impact of cybercrime is substantial and deserves attention and investments on cybersecurity in order to counter the increasing number of cyberattacks, however not all the economic sectors are hit in the same way, what emerged is that the highest cost of cybercrime is borne by the banking and utilities industries. Furthermore, as far as the geographical distribution of cyberattacks is concerned, the United States continues to top the list, with an increasing annual cybercrime cost of + 29% in 2018 (US$27.4 million), but other countries registered even an higher increase, organisations in the United Kingdom, for instance, registered an increase of +31% (US$11.5 million), followed by Japan with an increase of +30% in 2018 (US$13.6 million). While, other countries, like Germany, that have extensively invested in cybersecurity during the last year, observed a lower increase in 2018. Furthermore, considering Italy, the main targets of cyber-attacks are the public administrations, which registered in 2018 an increase of the attacks five time higher than the previous year (+561%), on the other hand the private sector is at risk as well, with attacks in 2018 to the telecommunication (6%), energy (11%) and transportation (6%) sectors as the main targets. Taking into consideration the origin of the cyber-attacks directed against the Italian security, the pattern for 2018 remains stable with that one of the previous year, registering 66% of the attacks directed by hacktivist groups, 20% being state-sponsored, 9% not identified and 5% attributable to terrorist groups.

---

[269] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Heaven, Connecticut: Yale University Press, 2018).
[270] UNODC, Comprehensive Study on Cybercrime, (New York: United Nations, 2013). Available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
[271] Accenture, *Ninth Annual Cost of Cybercrime Study*, 2019. Available at: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

As far as the types of attacks are concerned, the analysis showed how malware is the most frequent attack overall. The number of ransomware attacks, experienced by organisations, increases over the year by 15%, while the number of phishing and social engineering attacks increased by 16% in the last year (2018), highlighting that 85% of organisations experienced this type of attacks. Moreover, people-based attacks registered the largest increase over the year. This last information is interesting, since it showed us that people continues to be the weakest point in cybersecurity defence.

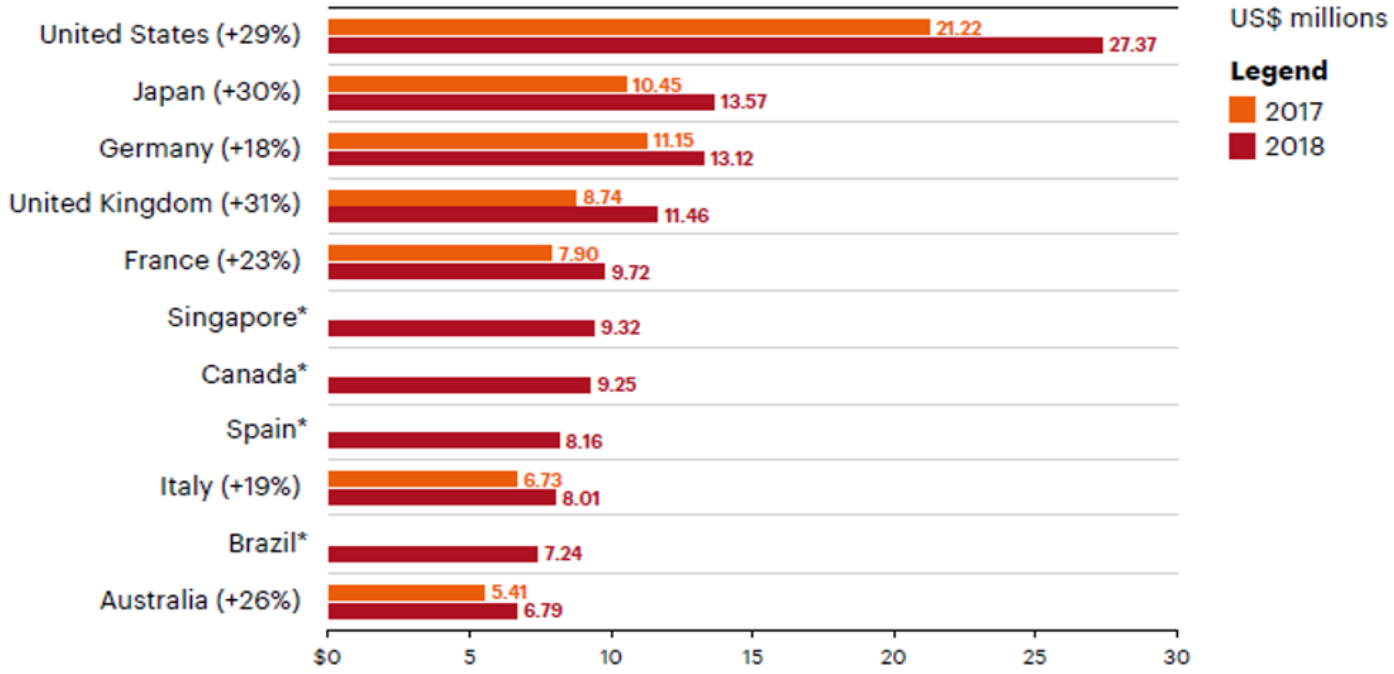
Fig.3 The average annual cost of cybercrime by industry



Source: Accenture, *Ninth Annual Cost of Cybercrime Study*, 2019.

Furthermore, the global cost of cybercrime is projected to increase over the next years and the total value at risk from cybercrime is estimated to be US$5.2 trillion over the next five years.[272]

Fig.4 The average annual cost of cybercrime per country



Source: Accenture, *Ninth Annual Cost of Cybercrime Study*, 2019.

According to a research conducted by the European Union Agency for Network and Information Security (ENISA) jointly with Computer Emergency Response Team for the European Union Institutions, bodies and agencies (CERT-EU), fifteen top cyber threats[273] have been detected:

1) malware: is the collective name for a number of malicious software variants (e.g. virus, worms, spyware, trojans, ransomware). It consists of a code developed by cyber attackers, designed to cause extensive damage to data and systems or to gain unauthorized access to a network. Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware. A global malware outbreak was caused in 2017 by WannaCry and Petya. Malware is the most frequently encountered cyberthreat, involved in 30% of all data breach incidents reported;[274]
2) web based attacks: they employ the web systems and services as a starting point for compromising the target. Among the different types, we can mention the drive-by, watering-hole, redirection and man-in

[272]Ponemon Institute LLC and Accenture, *The Cost Of Cybercrime. Ninth Annual Cost Of Cybercrime Study. Unlocking The Value Of Improved Cybersecurity Protection*, 2019. Available at https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.
[273]ENISA, *Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, Final Version 1.0 ETL 2018*, January 2019. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.
[274] Forcepoint, *What is Malware? Malware Defined, Explained, and Explored*, https://www.forcepoint.com/cyber-edu/malware.

the-browser attacks. They represent one of the most relevant threats and are expected to increase;

3) web application attacks: consist in the abuse of an active or passive component of a software available via web. The trend of attacks in 2018 registered a slight decrease, since enterprises and organisations are investing more on web applications detection, protection and defence systems;
4) phishing: it consists in crafting messages using social engineering techniques in order to cheat the receiving target. The phishers try to lure the recipients of phishing emails and messages to open a malicious attachment, release credentials, money or valuable information. Over 90% of malware infections and 72% of data breaches in organisations come from phishing attacks;
5) Distributed Denial of Service (DDoS): the mechanism of the attack is based on the capacity limits of any network resources. The DDoS attack sends multiple requests to the target web resource with the goal of preventing the website from functioning correctly, overwhelming it of requests superior to the website's capacity;[275]
6) spam: abusive use of email and messaging technologies to flood users with unsolicited messages. The main advantage of this attack is the low cost. It is expected to be still a threat in the near future due to its evolution within the social networks;
7) botnets: *crasis* of the words 'robot' and 'network', a bot is a piece of malicious software that gets order from a master. A system acquires the infection when a bot is installed by a worm or a virus, or when the user visits a malicious website. Cybercriminals seek to infect the highest number possible of computers (even millions) and take control of the systems acting remotely, becoming the masters of a 'bot-network', used to deliver DDoS attack or spam campaigns;[276]
8) data breaches: refer to the leakage or exposure to an unauthorized person of confidential, sensitive or protected information due to the actions of an accidental or malicious insider/outsider or to a lost or stolen device. Common attack methods employed are the following: stolen credentials, compromised assets, payment card fraud, third-party access and vulnerabilities associated with a 'bring your own device' (BYOD) policy of a company or organisation;[277]
9) insider threat: it is a very common threat for every company or organisation. It refers to the intentional or unintentional abuse of access to the organisation' digital assets, by a current or former employee, a partner or contractor. There are three main types of insider threats: the malicious insider acting intentionally and the compromised and negligent insiders acting unintentionally;
10) physical manipulation/ damage/ theft/ loss: refer to the risk of exposure of personally identifying information (PII). A strategy widely adopted by companies and organisation to reduce the risk of physical attack is to rely on storage encryption;

[275] Kaspersky, *What is a DDoS Attack? - DDoS Meaning*, https://www.kaspersky.com/resource-center/threats/ddos-attacks.
[276] European Union Agency for Cybersecurity, *B.otnets*, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets.
[277] Kaspersky, *What Is a Data Breach?*, https://www.kaspersky.com/resource-center/definitions/data-breach

11) information leakage: it relates to the substantial and reputational damage caused to a company or organisation in case of compromised information. The main causes are a technical failure or an individual responsibility;
12) identity theft: fraud committed from the theft of personally identifying information (PII). Main targets of this type of attack are bank account information, health records, personal web accounts and other personal information;
13) cryptojacking: also known as cryptomining, it refers to the process of using the target's device processing power (usually 70% to 80% of unused CPU or GPU[278]) to mine cryptocurrencies without consent. Cyber criminals earn real world money, monetized after legal exchanges and transactions;
14) ransomware: it is based on a mechanism which gains possession of files or devices and block the owner from accessing them, demanding a ransom in cryptocurrency as return. As pointed out by the 2018 Internet Organised Crime Threat Assessment (IOCTA),[279] even if the growth of this type of attack is decreasing, still represents the dominant threat in particular for the banking and financial sectors;
15) cyberespionage: also known as nation-state-sponsored espionage, it targets generally critical and strategic infrastructures – including governmental institutions, energy companies, telecommunication providers, transportations, banks, and hospital – with the main aim of stealing state and trade secrets and proprietary information in strategic fields.

Taking in consideration the current scenario, digital extortion appears to be the main threat for 2018 according to a research conducted by TrendMicro[280]. Organisations and private companies are exposed to the same risk of being targeted, in particular those working in an industrial Internet of Things (IoT)[281] environment, which are exposed to new and partially known vulnerabilities. Another challenge is that one placed by the implementation of the General Data Protection Regulation (GDPR), since cybercrime will employ social engineering to target data covered by the regulation and ask companies and/or organisation an extortion fee, which potentially the victims will pay to avoid the punitive measures provided by the GDPR for data breaches, which amount up to the 4% of a company annual turnover. Among the other trends described in the TrendMicro research, it is relevant to underline the persistent threat posed by disinformation, fake news and

[278] The Central Processing Unit (CPU) performs most of the processing inside a computer, controlling instructions and data flow to and from other part of the computer. It relies on hardware components called chipset, which is a group of microchips located on the motherboard.
The Graphics Processing Unit (GPU) is a programmable logic chip processor primarily used to manage and boost the performance of images, animations and video. GPU's are locate in a chipset on the motherboard or in the same chip as the CPU.
[279] EUROPOL, Internet Organised Crime Threat Assessment (IOCTA), 2018, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.
[280] TrendMicro and U.S. Secret Service Criminal Investigation Division (CID), *The Evolution of Cybercrime and Cyberdefense*, 2018. Available at https://documents.trendmicro.com/assets/white_papers/wp-evolution-of-cybercrime-and-cyberdefense.pdf.
[281] According to Cisco, *The Internet of Things*, The Internet Protocol Journal, Volume 15, No. 3: "The *Internet of Things* (IoT) consists of networks of sensors attached to objects and communications devices, providing data that can be analysed and used to initiate automated actions. The attributes of this world of things may be characterised by low energy consumption, auto-configuration, embeddable objects, etc. The data also generates vital intelligence for planning, management, policy, and decision making".

manipulation of political campaigns. As far as the countermeasures to fight cybercrime, a key role is that one played by the Public-Private Partnerships (PPP) based on information sharing, cooperation, technical prevention and protection measures, harmonisation of legislation, better cooperation between law enforcement authorities and the private sector.[282]

Fig.5 Overview and comparison of the threat landscape of 2018 with the one of 2017

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Source: ENISA, *Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, Final Version 1.0 ETL 2018,* January 2019.

[282] Presidenza del Consiglio dei Ministri - Sistema di Informazione per la Sicurezza della Repubblica, *Documento di Sicurezza Nazionale*, 2018. Available in Italian at http://www.sicurezzanazionale.gov.it/sisr.nsf/Relazione-2018.pdf.

3.2. Cybercrime and traditional organised crime: the group dynamics

When analysing cybercrime, it is necessary to consider the group dynamics within the phenomenon, in order to understand the structure characterising cybercrime in Russia. Traditional organised crime groups are increasingly expanding their activities in the cyber domain, taking advantage of the anonymity provided by the Internet, the low entry barriers and costs. Cybercrime groups and traditional crime groups present similarities, since the Internet can just be considered as another platform on which crime activities can be conducted, while the main difference lies in the relevance of technology for the development of crime acts and for the interaction among the members of a group. Choo and Smith[283] have identified three main ways in which traditional crime groups exploit the cyber domain. A first category involves those groups which exploit the Internet platforms to extend their conventional crime activities such as piracy, fraud and extortion. According to this analysis, criminals employ the cyber space as a business-service model, where the criminal can purchase illegal services such as botnets or customised malware in the Dark Web markets and easily put in place cyber-attacks like DDoS against their traditional targets.[284]

The second category refers to organised cybercriminal groups that exploit the Internet as the main platform for the planning and execution of their activities. One example of such a group is the Carbanak cybercrime group, also referred to as FIN7 and Navigator Group, active since 2015 and mainly targeting U.S. companies, stealing millions of customer credit and debit card numbers and sensitive information, which were later sold online. In 2018 Europol claimed to have arrested the main leaders of the group, the Ukrainian nationals Dmytro Fëdorov, Fedir Hladyr and Andrij Kopakov. Another relevant characteristic of organised cybercriminal groups is that they operate remotely and usually they never meet in real-life but only online, this is the case of the Lulzsec group, another black hat computer hacking[285] group responsible for the attacks against user accounts of Sony Pictures in 2011 and responsible for the shutdown of the CIA website. The third group identified by Choo and Smith is that one of ideologically and politically motivated cyber groups. This last category involves mainly hacking groups and terrorist organisations, which commit cybercrimes not as primary activities but just as an instrumental way to raise funds for their main objectives.

Another interesting aspect related to cybercrime is the analysis of the related platforms employed. Originally, cybercrime groups acted on platforms such as Internet Relay Chat (IRC), while more recently has been

---

[283] Choo Kim-Kwang Raymond and Smith Russell G., "Criminal Exploitation of Online Systems by Organised Crime Groups" in Asian Journal of Criminology 3(1):37-59 · June 2008. Available at https://www.academia.edu/33267677/Criminal_Exploitation_of_Online_Systems_by_Organised_Crime_Groups.

[284] Nurse Jason R. and Bada Maria, "The Group Element of Cybercrime: Types, Dunamics, and Criminal Operation" in *The Oxford Handbook of Cyberpsychology*, edited by Alison Attrill-Smith, Chris Fullwood, Melanie Keep, and Daria J. Kuss, (Oxford: 2018). Available at https://www.researchgate.net/publication/328763267_The_Group_Element_of_Cybercrime_Types_Dynamics_and_Criminal_Operations.

[285] Black hat hacking refers to the activity of exploiting computer security vulnerabilities for financial gain or generally malicious reasons, while, white hat hacking refers to IT security professionals employed by companies or organisations to find security flaws which could turn to vulnerabilities.

registered a widespread use of social networks (including Facebook), social media (among which MySpace, Bebo and Hi5), forums (e.g. Reddit, CraigList and 4Chan), apps and instant messaging services (including Whatsapp, WeChat, SureSpot, Kik, Wickr and Signal), which provide secure and encrypted communications. Moreover, another platform used by the cybercriminals and terrorists is the Dark Web, which is defined as "the part of the web which exists on an encrypted network and can only be accessed using specific software and networks, such as Tor (or, The Onion Router) and I2P (the Invisible Internet Project)".[286] Ideological hacking groups are those which are prone to be hired by a state, thus engaging not only in the traditional state-sponsored attacks such as espionage but also corporate theft and sabotage.[287]This category of hacking groups is expected to rise in the following years and it puts a huge threat to the international security system, since most of the governments are involved in the so-called nation-state cybercrime from the Russian Federation to the United States of America. Another issue worth mentioning is the fact that ideological hacking groups are difficult to control, given the fact that their main goal is not mere financial gain but a political or moral belief, which opens the question of whether or not they will be loyal to the government that "hired" them. As far as the way in which cybercriminal groups are organised is concerned, it is interesting to mention that their structure differs substantially from that one typical of traditional organised groups. In fact, cybercrime groups are not organised in a hierarchical way, rather their structure can be defined as a decentralised and distributed model of organisation. This aspect is relevant since the lack of a single leadership makes it difficult to comprehend the structure and the aims of the criminal organisation as well as the identification of the role played by each component. Moreover, what makes the analysis of cybercrime more complex, if compared to that one of traditional crime, is the identification of the reasons behind their actions. Some cybercrime groups share common characteristics with traditional crime in terms of the reasons of their actions, with financial gain being the main driver of their activities. Nevertheless, the vast majority of cybercriminals are not just moved by financial gain, rather the main motivators are political or religious beliefs, sexual impulses or even boredom and simple curiosity, as pointed out by Shinder.[288] Furthermore, another element worth mentioning is that cybercriminals, as argues Lusthaus,[289] can be protected by Russian traditional organised groups but more commonly are the law enforcement agents themselves or the political élite which protect them, in exchange of personal favours or payment. This *status quo* existing in Russia opens the discussion of another issue, that one of the connivance between the state apparatus and *Rossijskaja Organizacija*, including cybercriminals.

[286] Nurse Jason R. and Bada Maria, "The Group Element of Cybercrime: Types, Dunamics, and Criminal Operation" in *The Oxford Handbook of Cyberpsychology*, edited by Alison Attrill-Smith, Chris Fullwood, Melanie Keep, and Daria J. Kuss, (Oxford: 2018), p.3.
[287] Malwarebytes, The New Mafia: Gangs and Vigliantes. A Guide to Cybercrime for CEOs, 2017. Available at https://www.malwarebytes.com/pdf/white-papers/Cybercrime_NewMafia.pdf.
[288] TechRepublic, *Profiling and categorizing cybercriminals*, 2010. Available at http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069.
[289] Lusthaus Jonathan, *Industry of Anonimity: Inside the Business of Cybercrime*, (Cambridge: Harvard University Press, 2018).

3.3. Russian approach to cybercrime: the "criminal-governmental nexus"

When analysing the cyber domain, it is common to find in the literature a divide between the cyberwarfare and the cybercrime, with the first element linked to the nation-state security and defence. Nevertheless, analysing the Russian approach to the cyber domain, the hypothesis of the present research is that the line between cyberwarfare and cybercrime is not a definite one, rather it is quite blurred. The main reason that lies behind this hypothesis is the fact that information security and state control of the Internet are the Russian priorities, while for the West the main aims are the security of personal data and defence of the critical infrastructures. From this assumption a number of consequences can be listed, among which the fact that in the privacy-security pair, the Russians will certainly favour the second element. The State is still, in contemporary Russia, the core of the society, to which is asked to sacrifice themselves if needed. Moreover, this highlights also another aspect, the fact that for a superior aim, for the defence of the nation against the foreign powers which continuously try to destroy Russia (as stated in several official documents of the Russian Federation, such as the Doctrine of Information Security), it is reasonable to employ unconventional resources (cybercriminals) for the protection of the common good, of the collective wellness.

The Russian cyber challenge is not a new phenomenon, with the first embryonic cyberattacks against the West in 1986, particularly against the U.S. and West Germany, working in collaboration with the East Germany State Security Service (*Staatssicherheitsdienst*, SSD), commonly known as the *Stasi*. As argued by Popescu and Secrieru the origin of Russian cyber power lies in " […] its expertise in intelligence gathering as well as in Russian domestic politics".[290]In fact, Russia has begun developing a sophisticated cyber strategy through the exploitation of the military conflict in Chechnya during the 2000s, to combat the adversary's online campaigns and to suppress diverse Russian opposition groups within the national borders. Exactly from that military conflict, the first systematic disinformation campaigns were developed, alongside with the deployment of trolls and bots.[291] Moreover, at that time, started to develop another relevant issue, that one of the collaborations between the Russian State and the so-called *patriotičeskie chakery* ('patriotic hackers'), as defined by the President of Russian Federation Vladimir Putin those proxy cyber-activists which were supposedly involved in the interference in the 2016 U.S. elections. Not only Putin underlines the patriotic gesture committed by those hacking groups but he also added, during the same meeting with the heads of international news agencies in June 2017, that it is "theoretically possible" ("*teoretišeski eto vozmožno"*)[292] that they have acted in such a way, and the reason why is that they believed it was reasonable to defend Russia.

---

[290] Popescu Nicu and Secrieru Stanislav, *Hacks, Leaks and Disruptions. Russian Cyber Strategies*, (Paris: Chaillot Papers, European Union Institute for Security Studies, 2018). Available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf.

[291] A *troll* is defined as a member of an Internet community, who posts offensive and controversial comments with the aim of disorienting the public opinion. *Bots* are software applications or script which perform malicious tasks on command, used by hackers to take control of an infected machine remotely.

[292] Putin: khakerami mozhet dvigat' patrioticheskij nastroj, June 2017. Available in Russian at https://www.bbc.com/russian/news-40118501.

This statement is of the utmost importance since it publicly admits that the Russian state not only does not exclude the possibility of Russian-speaking cybercrime groups being involved in the internal affairs of a foreign state, but it also states that it is right and laudable to do it in the defence of the State. Moreover, the "criminal-governmental nexus", a syntagma used in the present research to indicate the connivance between the Russian state and hacking groups, is clearly visible in three episodes in which Russia was involved, namely the diplomatic clash with Estonia (2007) and in the military conflict in Georgia (2008) and Ukraine (2013-present), which have served as grounds to test Russian cyber capabilities and tactics. In the case of Estonia, DDoS (distributed denial-of-service) attacks were launched against Estonia's internet websites, forcing them to shut down and making the country unable to communicate and share information with the outside world. "The hackers appear to have been strategic in their choice of targets, attacking Estonian economic and political centres of gravity, including banks, ISP providers, telecommunications hubs, media outlets, and government websites. The cumulative impact of the attacks was the equivalent of a cyber blockade, in which Tallinn's internal and external communications links were degraded.", reported a research conducted by CNA's Center for Naval Analyses the federally funded research and development center (FFRDC) for the United States Navy and Marine Corps.[293] Estonian authorities claimed the attacks to be directed by Russians in retaliation for the decision to move a bronze statue of a Soviet soldier from its original position in Tallinn, a decision which was highly criticised by Russia and the ethnic Russians living in Estonia, considering it an outrage to the sacrifice of Soviet soldiers in the liberation of Estonia from Nazism. After the removal of the statue, violent protests followed, organised by ethnic Russians in Estonia. During the same period the first cyber-attacks were deployed. The effects of these attacks and their timing suggest they were part of a wider information operation campaign directed by Moscow. In the aftermath of the riots, in fact, the Russian Federation Council imposed economic sanctions to Estonia and diplomatic ties with the Baltic country were compromised. Another example, that clearly shows the close relation between the state apparatus of the Russian Federation and hacking groups is presented by the Russo-Georgia conflict in 2008. The origin of the confrontation laid in the pro-Western foreign policy pursued under the President Mikehil Saakashvili and the issue of the separatist republics of South Ossetia and Abchazia. The Russian military intervention in South Ossetia was coupled by extensive DDoS attacks against Georgia's governmental, economic and communication networks as well as telecommunication providers. A further example showing Russia's cooperation with hacking groups is that one of the on-going conflict in Ukraine, started in 2013, where an extensive and coordinated strategy has been applied with the aim of destabilising and disorientating the country, compromising the legitimacy of the Ukrainian political and military institutions as well as their capacity to operate and communicate. In Ukraine were tested not only the cyberattacks already employed in Estonia and Georgia, but for the first time, a country's electric power grid was a cyber-target. The attackers turned the distribution centres offline, using remote access to control and operate breakers and employing sophisticated cyber surveillance tool as

[293] Connell Michael and Vogler Sarah, Russia's Approach to Cyber Warfare, (Virginia: CNA Analysis & Solutions, March 2017). Available at https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

BlackEnergy to infiltrate the power centre networks. Moreover, always in Ukraine, it has been registered the deployment of an advanced cyber malware (Ouroboros) to open backdoors[294] in Ukrainian governmental systems. The advanced level of the attack perpetrated against Ukraine is a signal of the cooperation of the hacking groups with state intelligence or military agencies such as the GRU, the FSB and the SVR[295] The attack against Ukraine showed a common pattern with the others directed against Estonia and Georgia, that one of an Information Warfare operation, whose impact aims to destabilise and hit psychologically the opponent. All the three mentioned examples are useful when analysing the governmental nexus, since they show us the close ties of Russian hacking groups with the State.

The origin of the connection between the state security apparatus and the *Rossijskaja Organizacija* lies in the fall of the Soviet Union in the 1990s and the transition from the *vory v zakone* (thieves in law) to a new leadership of *avtoritiety* (authorities), which infiltrated the societal economic tissue, taking advantage of the privatisation waves enacted during the El'cin's era, the loophole in the legislative domain and the State's lack of control over the changes the society was undertaking. During this transitional phase organised crime evolved in Russia, abandoning the violence of street clashes among different groups and shifted towards a model based on targeted assassinations and collusion with corrupted state officials. This process not only revolutionised the criminal *milieu* in Russia but "it also led to a restructuring of connections between the underworld and the 'upperworld', to the benefit of the latter", as stated by Galeotti.[296] The result of this new deal was the creation of a "nationalised underworld"[297] in Russia which is compelled to comply to the Kremlin's requests. For instance, during the second Chechen War (1999-2009) Chechen criminal organised groups were convinced not to support their compatriots in the confrontation against Russia in view of a generous economic rewards. Moreover, under Putin's presidential mandate, organised crime is employed as an extension of the state's foreign policy, in the context of the widespread belief of the continuous threat placed by the West against the Russian Federation.

When considering the "criminal-governmental nexus" we need to analyse the approach of the law enforcement authorities towards cybercrime and the main finding is that there is a general weakness of the legislation on that subject and the unwillingness to properly punish cybercrime. In fact, if we analyse the Criminal Code of

---

[294] A *backdoor* is a technique employed to bypass the security system and obtain, without being detected, access to a computer system or network.

[295] *GRU* is the acronym of *Glavnoye Razvedyvatel'noye Upravleniye*, the Main Intelligence Directorate the Russian foreign military-intelligence agency, that, unlike Russia's security and intelligence agency is not directly subordinated to the president of Russia, but to the Russian military command, i.e. the Minister of Defence and the Chief of the General Staff.
FSB is the acronym of *Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii*, the Federal Security Service of the Russian Federation, the main Russian security agency, the successor agency to the *KGB*, an acronym of *Komitet Gosudarstvennoy Bezopasnosti*, the Committee for State Security, that was the main security agency for the Soviet Union from 1954 until its break-up in 1991.
SVR is the acronym of *Sluzhba Vneshney Razvedki Rossiyskoy Federatsii*, the Foreign Intelligence Service of the Russian Federation, focusing on civilian affairs.

[296] Galeotti Mark, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, (London: European Council on Foreign Relations, 2017). Available at https://www.ecfr.eu/publications/summary/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe.

[297] Ibidem.

the Russian Federation[298] (1996, amended in 2012), and in particular Chapter 28 *(Crimes in the Sphere of Computer Information)* the legislative weakness is clearly visible. Two articles of Chapter 28 refer to punishment for crimes committed in the sphere of computer information, art. 272 (*Illegal Accessing of Computer Information*) and art. 273 (*Creation, Use, and Dissemination of Harmful Computer Viruses*). In both cases the crimes are punished with a scale providing a maximum penalty consisting in the deprivation of liberty of up to three years (art.272) or four years (art.273) to the payment of a fine up to 200 thousand roubles (art.272) or 500 thousand roubles (art.273), which is respectively the equivalent of about €2.700 euros and €6.765 euros. Not exactly a severe punishment, considering the damages caused by a cyber-attack on a company or a governmental institution. Furthermore, as argued by Kadlecová,[299] given the nature of cybercrime, that is prominently transboundary, a tighter cooperation among the countries involved in cybercrime activities is required. A demonstration of the willingness of Russia in fighting cybercrime could be the signing of the Budapest Convention on Cybercrime under the Council of Europe (2001), but at the present moment this is unlikely to happen. However, Russia signed in September 2018 an agreement on "Cooperation in Combating Cybercrime" between the members of the Commonwealth of Independent States (CIS), to guarantee effective detection and investigation of cybercrime. This initiative is certainly a positive mark in the fight against cybercrime, but it is also a negative signal toward the international community, since it shows how Russia prefers, also in the cyber domain, to conclude agreements in the Eurasian regional framework, rather than the international or European ones.

Moreover, according to part of the academia, "Russia has an obligation to monitor and prevent trans-boundary cybercrime under the standard of due diligence",[300] that means an obligation under international customary law. Moreover, Russia has a clear obligation in terms of international law, since it is signatory of the Convention against Transnational Organised Crime (Palermo Convention, 2000). Nevertheless, the main problems in the compliance of Russia with these international obligations are the difficulty of proving direct attribution for cybercrime and cyberattacks on the one hand, and the already mention unwillingness of the Russian Federation to apply severe penalties on cybercriminals, due to the connivance, old as the Soviet times, between the criminal groups and the political establishment. Other evidences of weakness of the law enforcement authorities in Russia against cybercrime are provided by the analysis of Sukharenko,[301] who reported that the number of crimes committed in Russia by means of computer telecommunication

[298] Ugolovnyj kodeks Rossijskoj Federeatsii,1996 Available in Russian at http://ukodeksrf.ru/skachat-uk-rf and available in English at https://www.legislationline.org/documents/section/criminal-codes/country/7/Russian%20Federation/show.

[299] Kadlecová Lucie, *Russian-speaking Cyber Crime: Reasons behind its Success*, (The European Review of Organised Crime, 2015), p.104-121. Available at https://www.academia.edu/16548880/Russianspeaking_Cyber_Crime_Reasons_behind_Its_Success.

[300] Ortner Daniel, Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime, BYU L. Rev. 177 (2015). Available at: https://digitalcommons.law.byu.edu/lawreview/vol2015/iss1/7.

[301] Sukharenko Alexander N., *Russian ITC Security Policy and Cybercrime*, PONARIS Eurasia Policy Memo No.601, July 2019. Available at: http://www.ponarseurasia.org/memo/russian-itc-security-policy-and-cybercrime.

technologies increased from 1.300 in 2001 to 174.674 in 2018. Moreover, analysing the data for 2019 (until July), an increase of +53% was registered in comparison to 2018.

These alarming data are not coupled with a properly judicial enforcement. Always Sukharenko[302] reported in his analysis that in seventeen years (2001-2018), 18.333 cybercrimes (under Chapter 28 of the Russian Criminal Code) were detected by the law enforcement authorities, of which only 4.100 offenders were identified. Looking at the data for 2019 (until July), the dynamic is exactly the same, 1.139 cybercrimes were detected and only 111 persons were identified as responsible. The main reasons for the lack of prosecution for who commits cybercrime are: the transnational nature of the cybercrime and the difficulty to detect who is responsible for the commission of the crime, the evolution of the technical tools employed by cybercriminals, the lack of adequate ITC-training in the law enforcement field and the unwillingness of the Russian Federation to adopt an aggressive and severe measures against cybercrime. This inefficiency of the Russian law enforcement system obviously has consequence at the international level, since it is extremely difficult to capture and convict Russians involved in malicious hacking activities, due to the fact that cybercriminals enjoy of a relative immunity in Russia, as far as they do not act against national governmental entities. In return for such immunity, it is believed that cybercriminals work for Russian intelligence agencies. Since cybercriminals usually work remotely, it is impossible to detain them if based in Russia, detention can be applied only when they move abroad, but generally they choose countries which are not signatories of extradition treaties with the United States of America. Nevertheless, some recent U.S. successful prosecution of Russian cybercriminals can be mentioned, such as Maxim Senach, arrested in Finland in 2015 and sentenced in August 2017 to four years in a U.S. prison for stealing financial account credentials through the 'Citadel' malware. Another recent example is that on of Roman Seleznev, arrested in the Maldives in 2014 and sentenced in April 2017 to 27 years in prison in the U.S., for connection with the Carder.su, a criminal group focusing on fraud and theft of sensitive data, which caused US$169 million damage to 500 business and 3.700 financial institutions.[303]

Fig.6 Registered ITC Crimes in Russia (2011-2018)

Year	2011	2012	2013	2014	2015	2016	2017	2018
Number of crimes	7,974	10,227	11,104	10,968	43,816	65,949	90,587	174,674

Source: Main Information and Analysis Center of the Russian Ministry of Internal Affairs

[302] Ibidem.
[303] Ibidem.

3.4. Case study of the "criminal-governmental nexus": the Advance Persistent Threat (APT) groups

The U.S. National Institute of Standards and Technology (NIST) defines the Advance Persistent Threat (APT) as "an adversary that possesses sophisticated levels of expertise and significant resources which allows it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)."[304] As stated by a research of the Katholieke Universiteit Leuven (KU Leuven), the APT originally referred to cyber-attacks against military organisations, but, nowadays, APT are focusing mainly on civilian targets (companies and governments).[305] APT attacks are characterised by: specific targets and objectives, an high level of organisation of the attackers, adaptation to the defenders' countermeasures and long-term campaign of attacks.[306] As far as the attack model followed by an APT is concerned, six phases have been identified by the aforementioned research:

1. *reconnaissance and weaponization*: during this phase the attackers gather information about the target, employing opensource intelligence (OSINT) techniques and psychological manipulation methods (social engineering);
2. *delivery*: the attackers deliver the "exploits"[307] to the target directly, through social engineering tools like spear phishing[308] or indirectly, compromising a trusted third party;
3. *initial intrusion*: the third phase refers to the first time the attackers succeed in accessing the target's computer or network. The traditional *modus operandi* is to execute a malicious code that exploits a vulnerability in the target's system;
4. *command and control (C2)*: the attackers take control of the compromised computer, thus exploiting the network, setting in place a number of measures to avoid detection, such as the use of legitimate services and publicly available tools;
5. *lateral movement*: after having established a communication between the C2 servers and the compromised system, the attackers move inside the network, to collect valuable data;
6. *data exfiltration*: steal of sensitive information which is transferred, under encryption, to external location controlled by the attackers.

---

[304] NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*. Special Publication 800-39, 2010. Available at: https://www.nist.gov/publications/managing-information-security-risk-organization-mission-and-information-system-view.

[305] Chen Peng, Desmet Lieven, Huygens Christophe, "A Study on Advanced Persistent Threats" in De Decker B., Zúquete A. (eds) *Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science*, vol 8735. (Berlin, Heidelberg: Springer, 2014). Available at: https://link.springer.com/chapter/10.1007/978-3-662-44885-4_5#citeas.

[306] Ibidem.

[307] An *exploit* is a piece of software or a sequence of commands that takes advantage of a vulnerability in a system with the aim of gaining control of a computer system.

[308] *Spear phishing* is defined by Kaspersky as "an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer".

Nevertheless, the aforementioned classification in six phases is a simplification of the APT attacks. In fact, due to the high level of technological expertise employed and the sophistication of this kind of attacks, it is difficult to describe a fix pattern, since APT attacks are continuously evolving and adapting to new scenarios. A more comprehensive classifications is the so-called framework MITRE ATT&CK, that describes accurately over 80 Threat Actors and the APTs' *modus operandi* in the different phases of the attacks. According to the data gathered in this framework (until January 2019), have been identified: 11 tactics, 224 techniques, 328 software employed and three main platforms used (Windows, Linux, MacOS).[309]

What distinguishes the APT's threat from other cyber threats is the high level of organisation of the attack, that is specifically customised on the target, and the level of sophistication employed. Moreover, as pointed out by Ghafir and Prenosil[310], APTs are based on the so-called "zero-day exploits" (publicly unknown security vulnerabilities inside a software) and advanced offensive techniques such as social engineering. This aspect, combined with the huge economic damage caused by successful APTs' attacks, make them a high-level cyberthreat. Furthermore, due to the fact that the main aim of APTs is gathering information about an adversary, i.e. espionage, they are often recruited by governments. This is the case of the Russian government, that systematically employs APT groups to fulfil its own foreign policy objectives.

Russia's intelligence services employ APT attacks with the aim of gathering information and enable disinformation campaigns. Russian APT attacks are characterised by high level of technological expertise, huge financial resources and meticulous organisation and planning. The main targets of Russia's state-controlled APTs are governmental and supranational organisations, military institutions, science and research institutes. As far as the fields on which Russia is interested, we can mention the energy sector, foreign policy, military policy, humanitarian issues and the distribution of EU funds.[311]

Two APTs have been classified as controlled by Russia's intelligence services: APT 28 and APT 29.

APT 28 (also known as Fancy Bear, Tsar Team, Sednit, Pawn Storm, Sofacy, Group 74 and STRONTIUM) has been identified by security firms such as Fireeye, ThreatConnect and SecureWorks as a Russian-controlled ATP. The British and Estonian intelligence as well as the United States of America believe that this group is associated with Unit 26165 and Unit 74455 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Russia's military intelligence agency.[312] According to a FireEye report[313],

---

[309] For further information: Swisscom Ltd Group Security, *Cyber Security Report 2019*, (Switzerland: February 2019). Available at: https://www.swisscom.ch/content/dam/swisscom/en/about/company/portrait/network/security/documents/security-report-2019.pdf.res/security-report-2019.pdf.

[310] Ghafir Ibragim and Prenosil Vaclav, *Advance Persistent Threat Attack Detection: An Overview*, International Journal of Advancements in Computer Networks and Its Security – IJCNS, Vol.: Issue 4 [ISSN 2250-3757], 2014. Available at: https://www.researchgate.net/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview.

[311] Bundesamt für Verfassungsschutz, *Cyber Attacks Controlled by Intelligence Services*, 2018. Available at: https://www.verfassungsschutz.de/en/public-relations/publications/publications-cyber-defense/publication-2018-05-cyber-attacks-controlled-by-intelligence-services.

[312] Council on Foreign Relations, *Cyber Operation Tracker*. Available at: https://www.cfr.org/interactive/cyber-operations/apt-28.

[313] FireEye Threat Intelligence, *APT28: A Window into Russia's Cyber Espionage Operations?*, 2014. Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

APT 28 is likely active since 2000s, targeting mainly governments, military and security organisations of interest for the Russian government. Specifically, the main targets are: the Georgia's Ministry of Internal Affairs and the Ministry of Defence; Eastern European governments and security organisations; European security organisations such as the North Atlantic Treaty Organisation (NATO) and the Organisation for Security and Cooperation in Europe (OSCE).

Fig.7 Targets of APT26 operations (2017-2018)

Source: Symantec Corporation, 2018.

Among the key findings of the aforementioned research, it has been noticed that APT has steady evolved its malware, adapting to the changing scenarios, moreover, the coding techniques used by the APT 28 malware show a high level of technological expertise. Furthermore, a number of indicators suggest that the group consists of Russian speaking individuals, given the evidence that a significant component of APT 28 was compiled in Russian language. Another evidence for the Russian attribution is that over 86% of the malware samples attributed to APT 28 were compiled during working days (Monday to Friday) between 8AM and 6PM in the UTC+3 time zone, corresponding to the working hours in Moscow and St. Petersburg.[314]Among the recent targets of APT 28, we can mention the attacks in 2016 and 2017 against German governmental institutions and political parties and against the Democratic National Committee (DNC) during the 2016 U.S. presidential elections. The group was also accused of having hacked the World Anti-Doping Agency (WADA) in 2016. Moreover, as observed by the Symantec's analysis, the attacks on the U.S. DNC and WADA marked

[314] According to a research conducted by FireEye on evidences ranging from mid-2007 to September 2014.

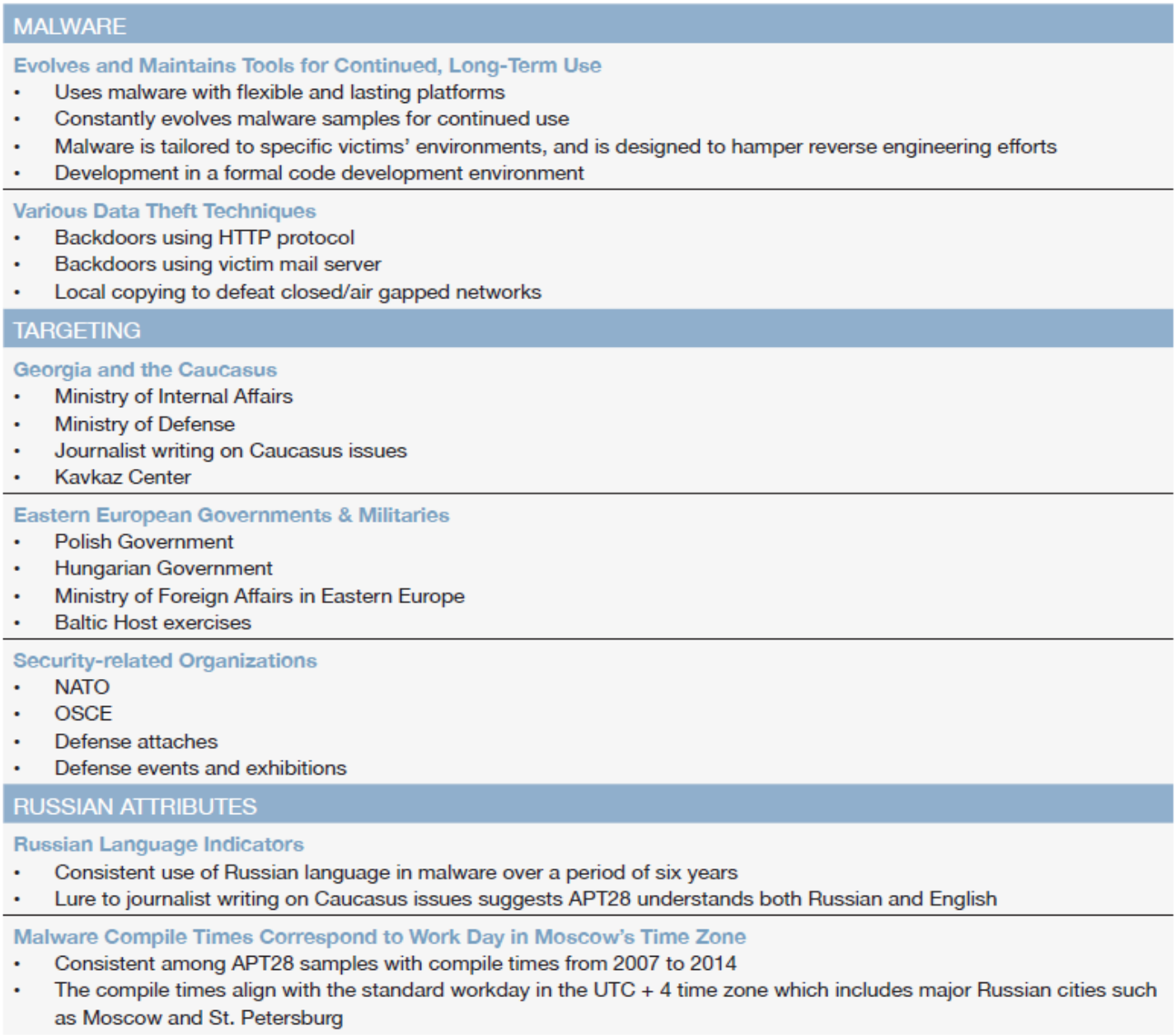
a turning point in the patterns of attacks followed by APT 28 and in the choice of the targets, shifting from low-key intelligence gathering to a more aggressive approach, with the aim of destabilising the targeted country.[315]As far as the methodology employed by the APT 28 group is concerned, the Cyber Kill Chain (CKC) model can be applied. The CKC, term originated in the military domain, refers to a systematic attack procedure composed of six phases. In the first phase (*Reconnaissance*) the APT28 identifies and profiles its target, by means of OSINT analysis and scan websites in order to find web application vulnerabilities. For example, Sandworm (also known as Microsoft OLE RCE CVE-2014-4114) is a vulnerability exploited by APT 28 to attack NATO, EU governments and Ukraine government. During the second phase of the CKC model (*Weaponisation*), the APT28, relying on the vulnerabilities found in the first phase, develops customised malware and uses social engineering techniques. At the practical level, they use spear-phishing campaigns or create fake links with a domain name similar to the original one and then induce the user to click on it.

Then, in the third phase (*Delivery*), the customised malware is sent to the targeted environment. In the fourth phase (*Exploitation*), APT28 uses zero-days exploits to trigger within the adversary system the intruder's code. APT28 uses different products for exploitation such as Adobe Flash Player, Microsoft Word, Java Runtime Environment and Internet Explorer. In the last case, APT28 exploits legitimate websites by injecting Browser Exploitation Framework (BeFF). In the fifth phase (*Installation*), malwares are installed in the adversary's computer system. Installation procedures and tools vary according to the operating system employed by the target. For instance, if the target is running macOS, ATP28 installs a backdoor trojan called xAgentOSx, while for a system using Windows, usually a bootkit infecting the Master Boot Record (MBR) is employed. In the final phase (*Command and Control*) a communication is established between the target and the Command and ContRol (C2) servers of ATP28.[316]

[315] Symantec, *APT28: New Espionage Operations Target Military and Government Organizations*, October 2018. Available at: https://www.symantec.com/blogs/election-security/apt28-espionage-military-government.

[316] Mwiki Henry, Dargahi Tooska, Dehghantanha Ali, and Choo Kim-Kwang Raymond Choo, *Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin*, (Switzerland: Springer, 2019). Available at: https://www.researchgate.net/publication/330071595_Analysis_and_Triage_of_Advanced_Hacking_Groups_Targeting_Western_Countries_Critical_National_Infrastructure_APT28_RED_October_and_Regin_Theories_Methods_Tools_and_Technologies/link/5ca3d8af458515f7851fcf4a/download.

Fig.8 Summary of key observations about APT28



Source: FireEye Threat Intelligence, *APT28: A Window into Russia's Cyber Espionage Operations?*, 2014.

The other Russia's controlled group is APT29 (also known as HAMMERTOSS, CozyCar, Office Monkeys, The Dukes and Cozy Duke). It is believed to be associated with the Russian Federal Security Services (FSB) and the Foreign Intelligence Service (SVR). FireEye cybersecurity firm analysed the APT29 since 2015 and argues that it is a particularly effective tool that employs different techniques (creation of algorithms which are applied daily to Twitter to embedding pictures with command). As in the case of APT28, the attribution to a Russian origin is assumed given a number of evidences, among which the fact that the targets and the information researched are of interest for the Russian Federation. Moreover, APT29 does not operate in periods corresponding to Russian holydays and their working hours align with the UTC +3 time zone, which

contains major Russian cities like Moscow and St. Petersburg.[317] Moreover, as for ATP28, also ATP29 is considered to be extensively involved in the hacking activities against the U.S. DNC during the 2016 U.S. presidential elections. Furthermore, the Russian attribution of APT29 is further strengthened by the targets chosen by the group, mainly in the administrative, defence, energy, Research and Development (R&D), and financial sectors. Another analogy with the APT28 is the high level of expertise showed by both APTs in terms of information technology, e.g. by exploiting zero-days vulnerabilities, and the extensive operational and analytical capacities.[318] If we consider the *modus operandi* employed by APT29, we discover that it acts by using common websites, such as Twitter, GitHub and cloud storage services, to send commands and extract data; visiting on a daily basis different Twitter handles automatically; communicating after a specific date (e.g. using timed starts); obtaining commands by means of images, which contain hidden and encrypted data; extracting information from compromised networks. APT29 is one of the most capable APT groups in terms of covering its tracks, since it systematically eliminates forensic evidences and shows a high degree of adaptability to the network defenders' security countermeasures.

3.5. The Russian cyberthreat: an assessment

Given the aforementioned analysis what emerges is that the Russian Federation, since the 2000s, consistently has implemented a sophisticated strategy of attack directed mainly towards the West and one of the battlefields employed is the cyber domain, in the framework of the Information Warfare (IW). In a continuously evolving world, the Russians demonstrated a high level of adaptability to the changing scenarios, in fact, relying on the traditional expertise and attention on scientific progress and innovation, they developed sophisticated cyber strategies and techniques. Moreover, an aspect worth mentioning is the perfect merger of the new technologies employed to launch the attacks and the old Soviet reasoning of the conspiracy of the West against Russia, tracing the lines of a new form of Cold War, that is played in the cyber domain as well. As discussed by Wirtz,[319]since Soviet times, espionage was directed towards strategic sectors relating to scientific innovations and military and technical information in the Western countries. As pointed out by Wirtz the Russians "[…] in their hearts, they are good Clausewitzians. In other words, they understand the paramount nature of politics in war. War is a political act. Its purpose is to alter the political judgments of opponents to better suit our own interests. Thus, to have a strategic effect, cyber power must be used in a way that will shape the political outcome of war. Russians are thus quick to think through the links between technology, military operations,

[317] FireEye Threat Intelligence, *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, 2015. Available at: https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html.
[318] Bundesamt für Verfassungsschutz, *Cyber Attacks Controlled by Intelligence Services*, 2018. Available at: https://www.verfassungsschutz.de/en/public-relations/publications/publications-cyber-defense/publication-2018-05-cyber-attacks-controlled-by-intelligence-services.
[319] Wirtz James J., "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy", Chapter 3 in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications, 2015). Available at: https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf.

strategy, and ultimately political outcomes, despite their lack of technological dexterity."[320] This is a key element, since, as observed in the present research, in the Russian mindset there is not a clear divide among the political, military and technological domains, as well as there is not a divide between cyberwarfare and cybercrime, with the latter being involved in the first category as showed in the aforementioned analysis. What emerges clearly is the evidence that Russia places the Information Warfare as a priority in the scenario of the 21th century, being aware of the relevance of data and information in contemporary world and being ready to exploit all the resources at its disposal to fight the war for the hegemony in the globalised world, engaging thus in an open confrontation with Western powers, especially with the United States of America. In this sense the 'criminal-governmental nexus' concept has been forged, with the assumption that this is a zero-sum game and Russia has no problem in using all the potential possible means to achieve its aims. For this reason, experts and even criminals in the cyber domain were recruited to launch sophisticated attacks against the West (e.g. APT28 and APT29). Another element which deserves attention, if we want to capture the origin of Russian cyber activities, is the fact that the cyber domain is totally included within the broader concept of Information Warfare (IW), which is multi-layered, consisting in intelligence and counterintelligence activities, as well as disinformation campaigns, debilitation of communication, psychological operations and propaganda. As stated by Smith "computers are among the many tools of Russian information warfare, which is carried out 24 hours a day, seven days a week, in war and peace".[321] Therefore, whenever analysing the impact or the origin of Russian-based cyber-attacks, would they be directed against governmental institution or private companies the main question we need to ask ourselves is how these attacks relate to the specific geopolitical and military context. Even in the case of traditional cybercrime activities, whose main goal is to gain financial resources, this aspect is not to be underestimated, given the fact that, as explained in the present research, there is in Russia a weird and accepted unofficial relation between the political establishment, if not the Kremlin itself, and the cybercriminals. Then, in order to understand and counter Russian-based cyber-attacks, we need to consider all these variables and the intersections among them, keeping in mind that Russian strategic culture is based on the political activity and the adaptation of the new technologies at disposal. Moreover, if we understand how the Russians think strategically, it will be easier to detect cyber-attacks and capture the real reason behind them. In fact, one relevant aspect, as already mentioned in the present research, is the merger between the old Soviet strategies and the new technologies. For instance, one element that became known in the analysis of Russian cyber strategies is the fact that attacks are not intended to destroy a target but just to undermine the adversary's strategy, to create confusion, to destabilise and to compel the target to focus on a specific damage caused by the attackers, that turns to be not the Russians' primary aim, rather the secondary one, allowing them to attack on their original primary goal, having distracted the adversary, that is fully engaged in defending the secondary target. This pattern of action has been observed in several Russian-based attacks against governments, international security organisations or private companies and it is nothing but the

[320] Ibidem, p. 32.
[321] Smith David J., *How Russia Harnesses Cyberwarfare*, Defense Dossier, Issue 4, August 2012, pp.7-8.

application of an old Soviet military principle called *maskirovka*, also known as Russian military deception. Roberts[322] explains the difference in the use of the traditional military principle, that lies in the fact that, while in the past it was employed on conventional battlefield, the new concept, a *maskirovka 2.0*, is used predominantly to achieve illegal political and geographical gains without engaging in an open military confrontation with the enemy.

[322] Roberts James Q., *Maskirovka 2.0: Hybrid Threat, Hybrid Response*, (Florida: Joint Special Operations University Center for Special Operations Studies and Research, December 2015). Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1007494.pdf.

V. THE EUROPEAN RESPONSE TO THE PHENOMENON OF ORGANISED CRIME

1. General overview

As observed by the Serious and Organised Crime Threat Assessment (SOCTA) report[323] realized by Europol, organised crime is a key threat to the European security architecture, with individual and organised criminal groups generating each year billions of euros in profits through the activities carried out within the European Union. Furthermore, organised crime in the last decade has acquired a fluid and flexible nature adapting to the continuously evolving societal structure. It has also become more sophisticated in the methods employed, renouncing to visibility and the use of violence and putting efforts to blend into the society without raising attention. In particular, the highest threat is represented by the infiltration within the legitimate economy, most notably in the financial and banking sectors, and in the political domain. Moreover, technological advancements and the spread of a multitude of communication channels had an impact on the society, triggering innovation and breakthroughs, as well as on the organised crime that has exploited to its own advantage the advances in technology, as demonstrated by the increasing number of cybercrime activities conducted in the last years in the European Union (EU), mainly in the economic and political domains, at detriment of the profits of legitimate business and the reputation of institutional bodies. Therefore, the fight against organised crime has been set as one of the key priorities of the European Union, which developed policies and partnerships to tackle the problem and to guarantee the European security.

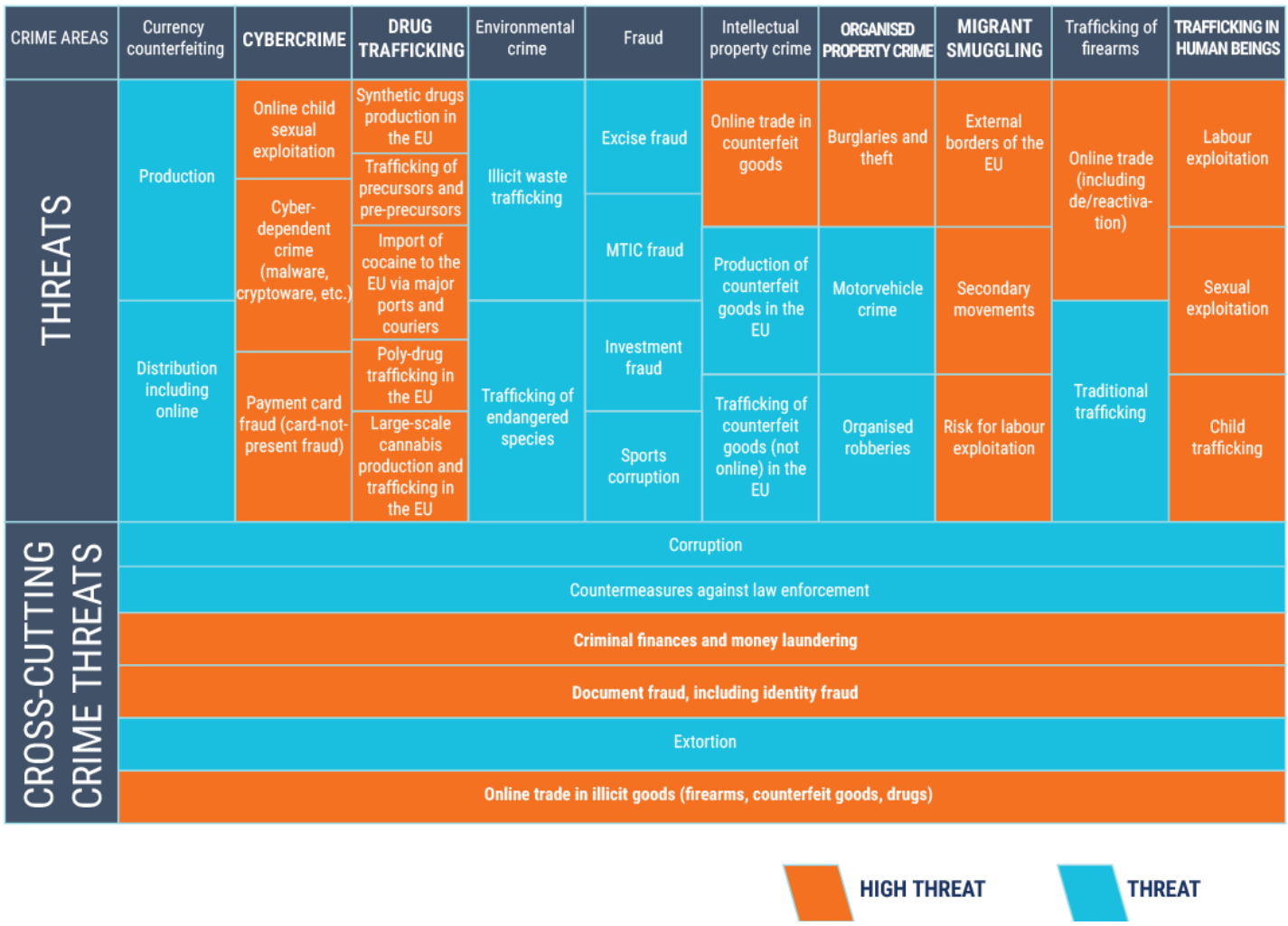
Based on the analysis conducted by Europol, five key priority threats to tackle serious and organised crime have been underlined, namely: cybercrime, drug trafficking, organised property crime, migrant smuggling and trafficking in human beings. Moreover, along with the aforementioned five specific criminal activities carried out by organised criminal groups in the EU, Europol has also recommended to focus on three cross-cutting threats which act as facilitators and enhancers of crime, namely: criminal finances and money laundering, document fraud and online trade in illicit goods and services.

In the following sections a comprehensive analysis of the measures adopted by the EU to tackle serious and organised crime will be analysed, providing the general framework of the main legislative tools and policies enacted to counter the problem. Moreover, two specific insights will be dedicated to the anti-money laundering initiatives and the measures to tackle cybercrime, due to the increased extension of the two related crimes within the EU in the last decade and due to the growing threats they place on the European security. In fact, crimes committed in the financial and cyber domains are considered to be the most relevant threat in the next

[323] EUROPOL, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017. Available at: https://www.europol.europa.eu/socta/2017/.

years, due to their nature and methods, continuously evolving and adapting to the changes and advancements of our societies.

Fig.1 Key priority threats for the European security



Source: EUROPOL, European Union Serious and Organised Crime Threat Assessment (SOCTA), 2017.

2. The European Agenda on Security 2015-2020

On 28 April 2015 the Commission adopted through a Communication[324] the European Agenda on Security 2015-2020, which defines the necessary measures to be undertaken at the EU level to counter the security threats to which the system is exposed. The Agenda constitutes the strategic framework for the implementation of the security measures within the EU and sets out the three main pillars for action in the security field where the EU can bring added-value: information sharing and exchange between national law enforcement authorities and the EU agencies; cooperation at the operational level; supporting actions (e.g. training and co-

[324] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security*, Strasbourg, 28th April 2015. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

funding). Moreover, in the Agenda three main priorities are outlined, namely: terrorism and radicalisation, serious and organised crime and cybercrime.

2.1. First Pillar: information sharing and exchange

Different tools have been developed to enhance and facilitate information sharing and exchange, among which the most widely known is the Schengen Information System (SIS), in operation in 26 EU Member States (only Ireland and Cyprus are not yet connected to SIS) and four Schengen Associated Countries (Switzerland, Norway, Liechtenstein and Iceland). SIS allows the national law enforcement authorities to consult alerts on targeted persons and objects. SIS comprehends measures related to the border control cooperation (Regulation (EC) No 1987/2006), law enforcement cooperation (Council Decision 2007/533/JHA) and cooperation on vehicle registration (Regulation (EC) No 1986/2006). As reported by the European Commission, at the end of the 2017 the SIS consisted of around 76.5 million records and it was accessed 5.2 billion times. Moreover, the system has been complemented by the establishment in each Member State of national SIRENE Bureaux, operating 24/7 and acting as focal points for the exchange of additional information and coordination pertinent to the SIS alerts. The main aim of the SIS is to guarantee the internal security in the absence of the internal border checks within the EU. The system underwent major changes in 2018 when a new SIS package has been approved and whose implementation in different stages will be completed by 2021. Different areas will be covered by the changes enacted, since the SIS will include biometric data such as palm prints, fingerprints, facial images and DNA; it will be accessed by the law enforcement authorities for preventive measures to protect specific categories of persons (e.g. missing persons, potential victims of trafficking in human beings); it will impact the migration field, since information about return decisions or entry bans will be incorporated in the system; it will include more information about persons involved in terrorism-related activities.

Moreover, in the context of the European Agenda on Security a set of common risk and border management indicators have been set to support law enforcement authorities and to prevent cross-border crime and terrorism, as well as complementary measures to monitor the movement of goods, tackling illegal trafficking of drugs, firearms and products smuggling at the borders. Then, an effective tool which requires increased implementation is represented by the Prüm framework, based on the Prüm Council Decision (2008/615/JHA) and the so-called Swedish Initiative (2006/960/JHA), the main legal instruments covered by the European Information Exchange Model (EXIM), adopted by the Commission in 2012. The Prüm framework guarantees operational police cooperation (e.g. joint patrols), automated comparison of biometric data among Member States and provides a common legal framework for the exchange of information and criminal intelligence between EU Member States' law enforcement authorities. This system is further complemented by other two mechanisms, the European Criminal Records Information System (ECRIS), that enables information exchange on previous convictions for EU nationals, and the European Police Record Index System (EPRIS), allowing access to national police records in order to enhance cross-border controls. A fundamental tool that enhances

the European security is also represented by the Europol's Secure Information Exchange Network Application (SIENA), which assures sharing and exchanging of information among Member States and third parties covered by cooperation agreements with Europol. Moreover, an effective measure to disrupt criminal networks has been represented by the EU Passenger Name Record (PNR) system for airline passengers, which allows to identify high risk targets in the context of drug trafficking, trafficking in human beings, child sexual exploitation and other serious crimes.

2.2. Second Pillar: cooperation at the operational level

At the operational level a pivotal role is played by the EU agencies, which contribute to the elaboration of security threats and risk assessments as well as common priorities for operational actions. Moreover, a number of cross-border tools have been developed at the EU level to enhance operational cooperation such as Joint Investigation Teams (JITs) on criminal cases, Joint Customs Operations (JCOs) to tackle cross-border crimes, cooperation between national Financial Intelligence Units (FIUs) and Asset Recovery Offices (AROs) to fight money laundering, the establishment of Police and Customs Cooperation Centres (PCCCs) in border regions and the judicial cooperation in criminal matters by means of the European Judicial Network (EJN) for the execution of European Arrest Warrants, assets freezing and confiscation.

2.3. Third Pillar: supporting actions

Training, funding and investments in research and innovation are fundamental to guarantee the European security. The effectiveness of the tools developed relies on the know-how of the law enforcement officers in the Member States. For this reason, common curricula on cross-border coordination and exchange systems are provided at the EU level in the European police college (CEPOL). Moreover, the Internal Security Fund has been created to address the main challenges up to 2020, provided of a strategic direction in order to fuel financial support where it will bring the most added value, according to the needs. Another relevant element is also represented by the investments in research and innovation in security-related domains, which is a fundamental aspect to effectively tackle the future security threats, that needs to be shaped in perspective of the law enforcements needs.

2.4. The priorities of the European Agenda on Security 2015-2020

Three main priorities have been identified by the European Agenda on Security 2015-2020, namely: terrorism and radicalisation, serious and organised crime and cybercrime. As far as the first priority is considered, for the present research, it is interesting to underline the efforts put by the EU to tackle the issue of financing terrorism, since there are evidences of profits made by organised criminal groups directly channelled into

terroristic organisations. Among the tools developed at the EU level, the cooperation of Financial Intelligence Units (FIUs) to track financial operations linked to terrorist networks is fundamental, as well as the EU-US Terrorist Financing Tracking Programme (TFTP), which allows Member States to access financial data of a target suspected of terrorist activity. Another mean at disposal to tackle the financing of terrorism is represented by the measures providing the freezing or confiscation of terrorist assets under Article 75 TFEU, the control of the forms of payments and the illicit cash flows. The second priority is devoted to combat serious and organised crime and involves different actions taken at the EU to counter the varied set of activities under the label of 'organised crime'. For the contrast of illicit drug trafficking the preventive measures are organised on the basis of the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), Europol's analyses and the EU Drugs Action Plan 2017-2020. While, for combating illicit firearms trafficking a common approach has been developed to neutralise and de-activate firearms to prevent their use by criminals. Moreover, the Commission has reviewed the existing legislation on firearms to enhance the information sharing and exchange, to strengthen traceability and establish common standards of marking and neutralisation of firearms. Considering smuggling of migrants, which represents a growing threat and destabiliser for the European security and cohesion, the EU has implemented in the last four years the European Agenda on Migration of 2015, promoting preventive action and coordination among Member States. Taking into account the trafficking in human beings, the Commission has communicated its commitment in 2017 to follow-up the EU Strategy towards the Eradication of trafficking in human beings 2012-2016, setting as main objectives the disruption of the traffickers' business models and the intensification of the cooperation among EU Justice and Home Affairs agencies, thus providing a comprehensive and coordinated response. Furthermore, in the fields of anti-money laundering and anti-corruption, which will be further analysed in the following sections, the EU agreed on an Anti-Money Laundering package in 2015, complemented in 2018 by the 5th Anti-Money Laundering Directive (Amendments to the 4th Anti-Money Laundering Directive), based on effective mechanisms to detect illicit money flows and shell companies as well as cooperation among the national Financial Intelligence Units (FIOs). Moreover, in the framework of the initiatives to counter financial crimes, a coordination with the national Asset Recovery Offices has been established, in order to improve freezing and confiscation of criminal assets as well as their mutual recognition.

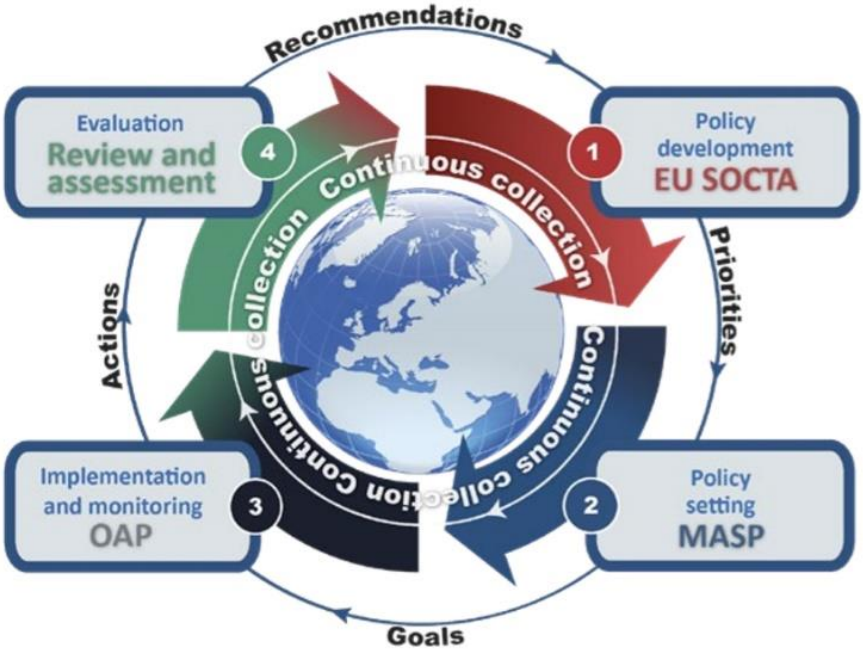
The third priority is represented by the fight against cybercrime, which is based on the 2013 EU Cybersecurity Strategy – whose main objectives are the identification of high-risk areas, the cooperation with the private sector and the realisation of specialised trainings for law enforcement officers – and the full implementation of the existing EU legislation, based on the 2001 Council of Europe's Budapest Convention on Cybercrime, and composed by: the 2013 Directive on attack against information systems, requiring Member States to improve national cybercrime laws and sanctions; the 2011 Directive on combating the sexual exploitation of children online and child pornography; the 2017 Directive implementing the 2001 Framework Decision on combating fraud and counterfeiting. Furthermore, the response to cybercrime must involve the coordination

among the Europol's European Cybercrime Centre (EC3), Computer Emergency Response Team for the EU institutions (CERT-EU), Eurojust and internet service providers.

3. The European Union Policy Cycle to tackle organised and serious international crime

The European Union commitment to tackle organised and serious international crime is shown by the adoption of the EU Policy Cycle, a four-years policy initiative launched for the first time in 2010 to provide a coordinate and more effective response to the threats placed by serious and organised crime. The management environment to carry out the objective set is the European Multidisciplinary Platform Against Criminal Threats (EMPACT), an evidence-based and multidisciplinary methodology designed to ensure cooperation among the law enforcements authorities of Member States, EU agencies and institutions and third parties at the national and EU levels, to provide a comprehensive action to counter the threats posed by organised criminal groups to the European security. The policy cycle is composed by four steps: the first one is the "Policy Development" through the EU Serious and Organised Crime Threat Assessment (SOCTA) realised by Europol, an analysis of the present and potential threats on the basis of the data provided by the Members States' law enforcement authorities, EU agencies such as the European Border and Coast Guard Agency (Frontex), Eurojust and European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), its own database and by third partner countries; the second phase is the "Policy Setting" with the choice of crime priorities and Multi-Annual Strategic Plans (MASP)", in which a four-years strategic plan is approved on the basis of a joint analysis made by the Standing Committee on Operational Cooperation on Internal Security (COSI), the Commission and the

Fig. 2 The EU Policy Cycle



Source: Council of the European Union, 2018.

Justice and Home Affairs (JHA) Ministers in the Council; the third phase is the "Policy Implementation and Monitoring", realised by means of the Operational Action Plans (OAPs) – drafted by Member States, EU institutions and agencies – and Drivers, tasked with the implementation of the OAPs and overseen by national coordinators; the fourth and final step is represented by the "Policy Evaluation" with the Commission review and interim assessment[325].

3.1. The EU Policy Cycle 2018-2021

On 18 May 2017, the Council of the EU adopted the EU Policy Cycle 2018-2021[326], where are listed ten key priorities for tackling organised and serious international crime between 2018 and 2021:

1. cybercrime: "to fight cybercrime, by (1) disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime, by (2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, and by (3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities"[327];
2. drug trafficking: "to (1) disrupt the activities of Organised Crime Groups (OCGs) involved in the wholesale trafficking of cannabis, cocaine and heroin to the EU, to (2) tackle the criminal networks involved in the trafficking and distribution of multiple types of drugs on EU markets and to (3) reduce the production of synthetic drugs and New Psychoactive Substances (NPS) in the EU and to dismantle OCGs involved in their production, trafficking and distribution"[328];
3. facilitation of illegal immigration: "to disrupt OCGs who facilitate illegal immigration by providing facilitation services to irregular migrants along the main migratory routes crossing the external border of the EU and within the EU, particularly focussing on those whose methods endanger people's lives, those offering their services online and making use of document fraud as part of their business model"[329];

[325] Council of the European Union – Standing Committee on Operational Cooperation on Internal Security (COSI), *EU Policy Cycle Terms of Reference*, Brussels, 5th December 2017. Available at: http://data.consilium.europa.eu/doc/document/ST-10544-2017-REV-2/en/pdf.
[326] Council of the European Union – General Secretariat of the Council, *Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021 - Council conclusions (18 May 2017)*, Brussels, 19th May 2017. Available at: http://data.consilium.europa.eu/doc/document/ST-9450-2017-INIT/en/pdf.
[327] Ibidem, p.6.
[328] Ibidem, p.7.
[329] Ibidem.

4. organised property crime: "to combat organised property crime by concentrating on disrupting highly mobile OCGs carrying out organised thefts and burglaries across the EU. This should include OCGs using new technologies or enhanced countermeasures which exploit the lacking interoperability of cross-border surveillance tools"[330];
5. trafficking in human beings: "to fight against the trafficking in human beings (THB) in the EU for all forms of exploitation, including sexual and labour exploitation as well as all forms of child trafficking"[331];
6. excise and MTIC fraud: "to disrupt the capacity of OCGs and specialists involved in excise fraud and Missing Trader Intra Community (MTIC) fraud"[332];
7. illicit firearms trafficking: "to disrupt OCGs involved in the illicit trafficking, distribution and use of firearms"[333];
8. environmental crime: "to disrupt OCGs involved in environmental crime, more particularly wildlife and illicit waste trafficking"[334];
9. criminal finances and money laundering: "to combat criminal finances and money laundering and facilitate asset recovery in view of effectively confiscating the criminal profits of OCGs, especially targeting money laundering syndicates offering money laundering services to other OCGs and those OCGs making extensive use of emerging new payment methods to launder criminal proceeds"[335];
10. document fraud: "to combat document fraud in the EU, targeting OCGs involved in the production and provision of fraudulent and false documents to other criminals"[336].

4. Europol: measures to counter serious and organised crime in Europe

As stated in the Strategy 2020, "Europol's mission is to support its Member States in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism."[337] To achieve its goal it has set five strategic priorities: be the EU criminal information hub, deliver agile operational support, be a platform for European policing solution, be at the forefront of law enforcement innovation and research, be the model EU law enforcement organisation.[338] Considering the first strategic priority, "be the EU criminal information hub", as pointed out in its Programming Document 2019-2021[339], Europol commits itself to develop advanced

[330] Ibidem.
[331] Ibidem, p.8.
[332] Ibidem.
[333] Ibidem.
[334] Ibidem.
[335] Ibidem.
[336] Ibidem.
[337] Europol Strategy 2020, Vienna, 13th December 2018. p.3. Available at: https://www.europol.europa.eu/publications-documents/europol-strategy-2020.
[338] Ibidem. pp. 4-6.
[339] Europol Public Information, *Europol Programming Document 2019-2021*, adopted by Europol Management Board on 30th November 2018, The Hague, 29th January 2019. Available at: https://www.europol.europa.eu/publications-documents/europol-programming-document.

ICT capabilities to maximise the exchange of criminal information. In this sense, it has elaborated a new integrated data management concept (IDMC), a decentralised system of information sharing tailored on the business needs of the law enforcement authorities and has implemented the first-line 24/7 information hub available to Member States to increase the quality and processing of information. In addition, to pursue its mission Europol promoted a multidisciplinary approach based on cooperation with a varied set of partners, including: EU agencies, such as Frontex and Eurojust, particularly in the field of irregular migration and cybercrime; cooperation with the European Union Agency for Law Enforcement Training (CEPOL), the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) and the Fundamental Rights Agency (FRA), mainly for initiatives in the Justice and Home Affairs matters and with the private sector and third partner countries (e.g. U.S., Balkan countries, Middle East and North African countries) as stated in the Europol External Strategy 2017-2020[340].

Taking into account the second strategic priority, "Deliver agile operational support", Europol put efforts to provide effective operational support to Member States in the three priority areas set out in the European Agenda on Security, namely serious and organised crime, cybercrime and counterterrorism. Particularly, Europol increased the intelligence sharing among Member States, supporting joint intelligence investigations and providing specialised forensic and technical support with long-term deployment of Europol experts to the European External Action Service (EEAS) and providing situation centres to coordinate the response to security crises. Moreover, Europol increased the operational results in the cybercrime domain, through the European Cybercrime Centre (EC3) and focalised on the disruption of serious and organised crime networks operating in the migrant smuggling activities, founding in 2016 the European Migrant Smuggling Centre (EMSC). Moreover, in the contrast to serious and organised crime Europol provides support in tackling poly-crime and mafia-type organised criminal networks, with a specific focus on illegal drugs and firearms trafficking, trafficking in human beings, organised property crime and cybercrime.

As far as the third priority is concerned, "Be a platform for European policing solution", Europol is committed to effectively coordinate its resources and to ensure the highest standards in terms of accountability and governance, in order to achieve its mission and to present itself as a trusted partner in EU policing in promoting and advancing the activities of the European law enforcement authorities. It aims to develop a common methodology and standard of analysis, an inventory of skills at disposal of the Member States' law enforcement authorities to promote best practices, as well increasing the visibility of the results obtained through the EU law enforcement cooperation.

Furthermore, to accomplish the fourth strategic priority, "Be at the forefront of law enforcement innovation and research", Europol has become a fundamental contact point for law enforcement authorities, developing innovation strategies and research hubs, necessary to counter the challenge of the increasing sophistication of crime, especially in the cyber domain.

[340] Ibidem. pp. 18-21.

Considering the fifth and last strategic priority, "Be the model EU law enforcement organisation", Europol achieves this goal by transparent and compliant management of resources, new and more effective communication strategies focused on the outcome of the joint operations deployed and through the strengthening of the available capabilities and human resources assets.

4.1. Combating serious and organised crime

The main operations of Europol to counter the threat of serious and organised crime are deployed through the European Serious and Organised Crime Centre (ESOCC), which provides intelligence analysis and support, monitoring of information flows, identification of High Value Targets (HVT) and establishing Operational Task Forces targeted on specific HVT; close cooperation with national investigators through Mobile Offices and Mobile Forensic Kits and implementation of the EU Policy Cycle and the related Multi Annual Strategic Plans (MASP) and Operational Action Plans (OAP). Overall, in 2018 the ESOCC supported 612 operations and provided over 3.445 analysis related to serious and organised crime[341]. Specifically, the ESOCC focuses on commodities and organised crime networks including operations on drugs, high threat organised crime groups and operations on weapons and explosives; economic and property crime including operations on fraud and counterfeiting; migrant smuggling and trafficking in human beings. In the fight against illegal drug trafficking Europol carried out 148 operations in 2018 and 200 operations have been targeted in 2019, based on close cooperation with representatives of the EU Member States, EU Commission, Eurojust, European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and the national law enforcement agencies (LEAs). Moreover, in the field of illegal firearms trafficking, Europol deployed 56 operations in 2018 and 80 targeted operations in 2019. Considering economic and property crime, Europol supported 204 operations in 2018[342] and developed new tools to enhance the response to those crimes, such as the identification of Alternative Banking Platforms (ABPs) used to funnel the proceeds of fraud out of the EU, the development of new initiatives related to the utilisation of biometric technologies based on facial recognition to identify members of criminal networks and providing new mechanisms to counter property crime such as Forensic Aid for Vehicle Identification (FAVI). Furthermore, the efforts of Europol are concentrated in combating migrant smuggling and trafficking in human beings, particularly through the European Migrant Smuggling Centre (EMSC), which supported 134 operations in 2018 and provided intelligence analysis and analytical support, cooperating closely with the Europol Mobile Investigation Support Teams (EMIST) and the Europol Mobile Analytical Support Teams (EMAST).

[341] Ibidem. p. 54.
[342] Ibidem.

5. Anti-money laundering measures

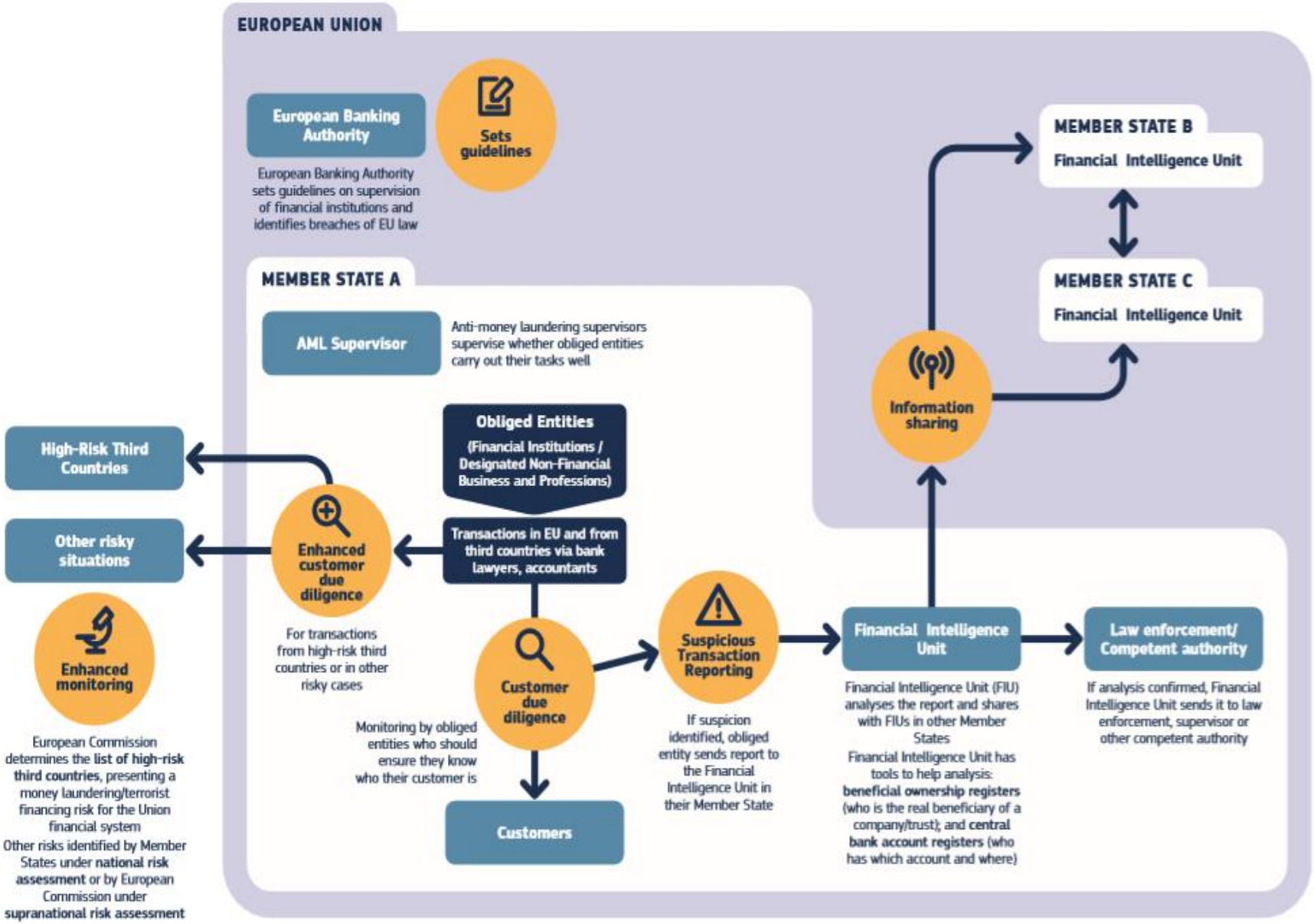
One of the most relevant threats to the European security architecture is represented by money laundering flows, as demonstrated in the present research by the case of the "Russian Laundromat" (for further details see ch.3). The development of effective anti-money laundering measures and the cooperation among the European Union countries in the financial and banking systems, as well as the advancement of the transparency and accountability standards in the EU are necessary steps towards the reduction of money laundering crimes and to counter the overall infiltration of organised crime groups within the European legitimate economy.

5.1. European Anti-Money Laundering Standards

In 1991 the European Union adopted the first Anti-Money Laundering Directive (AMLD), on the basis of the Financial Action Task Force (FATF) 40 recommendations of 1990, whose aim was to guarantee the stability of the Single Market and of the financial system. In 2005 a major reform was introduced with the adoption of the 3rd EU AMLD, that established a new architecture to fight money laundering, based on the Risk-Based Analysis (RBA) System, thus placing increasingly importance to the role played by the banking and financial institutions. A further progress has been made in 2015 with the adoption of the 4th EU AMLD, strengthening the cooperation, information exchange and transparency among Member States. Moreover, in June 2018 the 5th EU AMLD was adopted, introducing substantial amendments such as the setup of central bank account registers in all Member States and publicly available registers for companies, the improvement of powers of the EU Financial Intelligence Units (FIUs), the increased cooperation between anti-money laundering supervisors and the European Central Bank (ECB), and the limitation of the degree of anonymity guaranteed by pre-paid cards and virtual currencies. The 5th EU AMLD represents a turning point for the European Anti-Money Laundering System, nevertheless the major problems are linked to the different degrees of implementation of the directive in each Member State, as observed by the European Commission[343]. Moreover, the EU has established specific bodies dealing with anti-money laundering policies such as: the Expert Group on Money Laundering and Terrorist Financing, that assists the Commission in the definition of policy and drafting of new legislation, together with the Committee on the Prevention on Money Laundering and Terrorist Financing; the EU Financial Intelligence Units (FIUs) Platform, providing advice and expertise to the Commission; the Commission Expert Group on electronic identification (eID) and remote Know-Your-Customer (KYC) processes, gathering experts from the private and public sectors to provide advices and expertise.

[343] European Commission – Press Release, *Fight against money laundering and terrorist financing: Commission assesses risks and calls for better implementation of the rules*, Brussels, 24th July 2019. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452.

Fig.3 Preventing money-laundering activities in the EU



Source: European Commission, 2018.

6. Measures to counter cybercrime activities

The continuous evolution of technologies represents a specific feature of the contemporary society, creating both opportunities and risks. As analysed in Ch.4, one of the main risks associated with the cyber domain is that one of cybercrime activities directed against European institutions as well as private companies. Therefore, securing network and information systems in the EU is fundamental to guarantee the maximisation of the opportunities brought by the technological advancement and, at the same time, the minimization of the risks towards which the system is exposed.

The EU Cybersecurity strategy, launched in 2013 by the Commission and the European External Action Service (EEAS), represents the guideline for the European action in the cyber domain. It sets five priorities: the improvement of cyber resilience, the reduction of cybercrime, the elaboration of an EU cyber defence policy, the development of industrial and technological resources for cybersecurity and the establishment of an international cyberspace policy for the EU. Moreover, the commitment to fight cybercrime was renewed by the European Agenda on Security 2015-2020, as already discussed in the present research, where cybercrime is placed as one of the three main European security priorities.

At the legislative level, the cornerstone of the EU legislation on cybersecurity is represented by the Directive on Network and Information Security, also known as NIS directive (EU Directive 2016/1148), adopted in July 2016 and relying on three main pillars: the Member States' preparedness to be appropriately equipped to face cyber threats, requiring them to establish Computer Security Incident Response (CSIRT) and a national NIS Authority; the effective cooperation among Member States, by means of a Cooperation Group and the CSIRT Network; the establishment of a culture of security in strategic economic sectors such as banking, digital infrastructures, energy, financial market infrastructures, healthcare, transport and water[344].

Moreover, a number of networks and organisations have been created to guarantee security in the cyber domain, among which the most relevant is the European Union Agency for Network and Information Security (ENISA), which was set up in 2004 and whose main activities are: the collection and analysis of data on security incidents in the EU; the elaboration of risk assessment and risk management methodologies to improve the response against cyber threats; the support to the Computer Emergency Response Teams (CERTs) of the Member States; the cooperation among the different actors involved in the security field. Another relevant institution in the fight against cybercrime at the EU level is represented by the Europol's Cybercrime Centre (EC3), set up in 2013, which represents a reference point for tackling and preventing cross-border cybercrime. The EC3 constitutes a criminal information and intelligence hub which supports at the operational and investigative levels the Member States, providing high level technical and forensic capabilities as well as operational analysis and expertise.

[344] European Commission, *EU cybersecurity initiatives. Working towards a more secure online environment*, Brussels, 2017.

Notwithstanding the relevant progress realised in the cyber domain, there are still areas which need improvements. Among the deficiencies in the European cybersecurity scheme, there are for instance, the inconsistent transposition of EU law in the Member States as well as the cooperation between the different actors involved in the information exchange and the rapid detection and response to the threats[345]. Moreover, a fundamental aspect that needs further implementation is also represented by the Public-Private Partnerships (PPPs) against cybercrime, whose aim is to develop permanent and efficient information sharing channels, thus providing feedback on the investigations conducted, IT best practices and information on protection measures and new *modus operandi* employed to deliver the cyber threats[346]. Furthermore, new challenges are emerging to which the EU needs adequate preventive measures, such as the advent of the 5G technologies and artificial intelligence which will act as triggers and facilitators of cybercrime activities.

7. Recommendations to counter organised crime in Europe

Organised crime undermines governance, political stability and economic wellness in Europe. As analysed in the present research, the main trend observed has been that one of the increasing involvement of organised criminal groups in the European legitimate economy, through investment in strategic economic sectors and establishment of money laundering schemes. Another trend observed in the last years is also the enhanced capabilities developed by organised crime in the cyber domain to carry out high-level operation against financial or political targets. Taking in consideration the discussion pursued in the present research, the following policy recommendations should be taken into consideration to tackle the problem of the infiltration of organised criminal groups in Europe:

- further cooperation among European countries' law enforcement authorities due to the transnational character of organised crime in Europe;
- elaboration of common regulations over online platforms and applications, which are employed as facilitators for the activities of criminal groups, due to the weaker control in comparison with the level of regulation over the traditional financial service providers.

Considering drug trafficking:

- increased control should be applied to Belgium, Spain and the Netherlands, main entry points in Europe for cocaine trafficking;

[345] European Court of Auditors, *Challenges to effective EU cybersecurity policy*, Luxembourg, 2019.
[346] TrendMicro and U.S. Secret Service Criminal Investigation Division (CID), *The Evolution of Cybercrime and Cyberdefense*, 2018. pp. 31-32.
Available at https://documents.trendmicro.com/assets/white_papers/wp-evolution-of-cybercrime-and-cyberdefense.pdf.

- enhanced supervision in the European terminal points of the heroin-routes, such as: Bulgaria and Croatia for the “Classic Route”; Romania, Hungary, Austria and Slovakia for the “Northern Route”; Greece and Italy for the “Southern Route”;
- in the fight against production of synthetic drugs and new psychoactive substances (NPS), further regulations should be applied to Belgium and the Netherlands, which result the main production points in the EU.

Considering migrant smuggling:

- further communitarian funds must be allocated in European joint operations in the Mediterranean Sea to counter migrant smuggling, where most of the smuggling routes take place (Central/Eastern/Western Mediterranean routes);
- enhanced control over the European Union’s Eastern border (including Norway, Finland, Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Bulgaria and Romania).

Taking into account the trafficking in human beings (THB):

- higher control and regulation over the most targeted economic sectors employed by organised crime groups to deploy THB’s activities, namely: agriculture, cleaning services, construction, transportation);
- specific attention should be placed in Slovenia, Hungary, Estonia, Croatia and Denmark for the sexual exploitation, while in Malta, Portugal, Czech Republic and Belgium for labour exploitation.

Taking into consideration the illegal trafficking of firearms:

- elaboration of common standards for the reactivation of deactivated firearms;
- monitoring over illicit online market platforms (e.g. Dark web) where firearms are purchased;
- stricter control over the traffics from the Balkans, main origin countries of firearms, toward the EU.

Considering cybercrime:

- enhance common cybersecurity standards for both public and private organisations;
- monitoring online platforms and applications used for new payment methods (e.g. cryptocurrencies) and online illicit markets;
- effective implementation of the General Data Protection Regulation (GDPR) in all Member States of the EU.

8. Specific recommendations to fight the *Rossijskaja Organizacija* in Europe

The threat placed by the *Rossijskaja Organizacija* to the European security needs to be considered as one of the most challenging in the fight against organised crime. As observed by Galeotti[347], the role of the Russian organised crime in Europe has considerably changed over the past twenty years, renouncing to street violence and high visibility and becoming increasingly more integrated into the legitimate economic markets of the European countries as well as infiltrating the political domain.

The following policy recommendations should be taken into consideration to counter the infiltration of the *Rossijskaja Organizacija* in the European Union:

- not underestimating the threat posed by the phenomenon, whose level is particularly high also due to the large Russian-speaking communities within EU countries (e.g. Baltic countries, Germany) and their high level of assimilation;
- focusing on the financial and banking systems, in which the continuous evolution of the technological tools at disposal in the cyber domain have been exploited to deliver new and ever-changing patterns of attack;
- a specific attention should be placed on money laundering activities in the EU), particularly in the Nordic and Baltic countries, preferential sites for the operations deployed;
- the establishment of an effective mechanism to demonstrate the owners of specific structures and capital invested in the EU as well as the clear origin of the money flow;
- a common European approach against money laundering activity, as pointed out by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority in 2017[348];
- a particular attention and supervision should be placed by the EU institutions over those countries where there have been evidences of major investments made by the *Rossijskaja Organizacija* (e.g. Latvia and Cyprus);
- imposition of fines to pressure and incentivise continual surveillance by the banks themselves and enhanced inspections and government regulation, to overcome the gap in the EU anti-money laundering scheme represented by the banking system, since the banks are reluctant to report all the suspicious transactions;
- increased level of transparency and cost estimation related to project management and investments in the EU involving Russian counterparts;

[347] Galeotti Mark, *Crimintern: How the Kremlin uses Russia's criminal networks in Europe*, European Council on Foreign Relations, April 2017.

[348]European Banking Authority, *Final Guidelines on Risk Factors*, JC 2017 37, 26th June 2017. Available at: https://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf.

- heightened attention should be placed on the Russian expatriate communities in the EU, which must be considered a priority area for security, as underlined by Galeotti[349]. Law enforcement authorities should have a better knowledge of those communities, as well as cultivating relationship with them as allies and sources for the intelligence;
- assiduous monitoring of the European prisons system should be implemented, since it is exactly during the conviction period that new members are recruited by Russian organised criminal networks;
- the establishment of dedicated units within the police agencies in the EU countries most affected by activities carried out by Russian criminals, on the model of the Russian/Eurasian crime units within the France's *Office centrale de lutte contre le crime organisé (OCLCO)*;
- the creation in the EU of a cross-departmental body focused on Russian organised crime within Europol will assure a higher degree of effectiveness, particularly through specific cooperation with the financial intelligence and strategic operations departments;
- the strengthening of the relationships and cooperation with Moscow is required, especially on common areas such as the borders around Kaliningrad and along the border between Finland and Russia;
- higher degree of cooperation among European and Russian investigative agencies;
- enhanced cybersecurity standards for public and private organisations as well as monitoring social networks to detect botnets operations targeting political campaigns or initiatives.

Then, considering the case studies analysed (Germany, Italy, Latvia, Estonia and Lithuania), specific policy recommendations can be listed.

Considering Germany, the following measures to counter the infiltration of the *Rossijskaja Organizacija* should be applied:

- law enforcement authorities should focus on the cities of Cologne, Düsseldorf, Frankfurt and Hamburg, where the main concentration of Russian organised groups have been registered;
- particular attention should be placed on cybercrime activities (52.9% of crimes committed by Russian-speaking criminals in 2017 in Germany), through stricter control over the Internet, specifically monitoring the Internet underground markets (e.g. Darkweb, Deepweb);
- an effective approach should avoid focusing on just one ethnicity (e.g. Russians), since one of the main characteristics of the phenomenon is the high degree of collaboration with autochthone organised crime groups and foreign organised groups based in Germany.

[349] Ibidem.

As far as Italy is concerned, the following measures to counter the infiltration of the *Rossijskaja Organizacija* should be taken in consideration:

- higher control on the Northern regions, specifically in Emilia Romagna, Marche, Tuscany and Veneto in the real estate, food and beverage, tourism and gambling sectors;
- focus over the Apulian region, especially the city of Bari, where has been registered an extensive network belonging to the Georgian organised crime (*Kutaisi*, *Tbilisi* and *Rustavi* clans), mainly involved in property crime, drug trafficking and exploitation of prostitution;
- strengthening border and coastal controls always in the Apulian region, due to the presence of a systematic network of Ukrainian smugglers;
- tighter controls on the borders to allow the entrance of Ukrainian and Georgian nationals (since 2017 they are allowed to travel visa-free in the Schengen area up to 90 days within any 180 day period in[350]);
- employment of interpreters, by the law enforcement authorities, of the Russian, Ukrainian and Georgian languages with specific knowledge of the criminal crypto language (*fenya*), thus providing a better knowledge and understanding of the criminal group's strategies and targets;
- confiscation of assets, including shell companies, originating from illicit activities.

Taking into account the Baltic countries, the following measures are expected to counter the presence of the *Rossijskaja Organizacija*:

- considering the *Rossijskaja Organizacija* as an indigenous problem and not as an exogenous one, due to the historical presence of large communities of ethnic Russians in Estonia, Latvia and Lithuania;
- increased attention should be devolved to the cyber domain, in which the branches of the *Rossijskaja Organizacija* are concentrating their activities in the Baltic countries, specifically in the financial and economic sectors;
- monitoring of investments in the real estate market, preferential target for the money laundering schemes;
- enhanced control over the Riga port, a central hub for drug trafficking and smuggling of goods from Russia, due the connection with the port of St. Petersburg;
- tighter control on the border between Lithuania and the Russian exclave of Kaliningrad, one of the entry points in Europe of illicit drugs and smuggling of goods.

[350] Schengen VisaInfo, *Georgian citizens can travel to the Schengen Zone without a visa*, 27th March 2017. Available at: https://www.schengenvisainfo.com/news/georgian-citizens-can-travel-to-the-schengen-zone-without-a-visa/.
European Commission, *European Commission welcomes the Council adoption of visa liberalisation for the citizens of Ukraine*, Brussels, 11th May 2017. Available at: https://europa.eu/rapid/press-release_STATEMENT-17-1270_en.htm.

Then, an element of the highest relevance in the context of the fight against Russian organised crime is represented by “knowledge”, since the *Rossijskaja Organizacija* cannot be understood, neither defeated without knowing its origin, evolution and “culture”, in which reside exactly the reasons why it moves in a given territory, acquires a specific company or invests in a defined range of business sectors.

CONCLUSIONS

In this thesis I have tried to highlight the threat placed by organised crime to the European security architecture, specifically analysing the case study of the infiltration of the *Rossijskaja Organizacija* in Europe. According to the research conducted, the most challenging threat for the European security is represented by the criminal operations conducted within the boundaries of the legitimate economy, rather than the activities related to the illicit markets. In particular, the sectors which result to be most exposed to the threat of organised crime are the financial and banking sectors.

In order to demonstrate the relevance of the activities perpetrated within the European legal markets by organised crime, the case study of the *Rossijskaja Organizacija* has been extensively analysed and a set of concluding remarks have been proposed in the present research to underline the threat placed by the *Rossijskaja Organizacija* in Europe.

Concluding remark I: the specific nature and structure of the *Rossijskaja Organizacija* cannot be completely associated with mafia-like structures; thus, the countermeasures should be developed according to this assumption.

In order to analyse accurately a phenomenon it is necessary to define it, for this reason a specific terminology has been formulated in this thesis, namely that one of *Rossijskaja Organizacija*, that the author finds as the most accurate to describe the object of the research. The first term, "*Rossijskaja*", comes from the Russian adjective "*rossijskij*", which refers to something belonging to Russia, to the State, without placing the attention on the ethnicity as the term "*russkij*" in other expressions employed in the scientific literature to describe the phenomenon, such as "*Russkaja mafija*". The phenomenon of the *Rossijskaja Organizacija*, as explained in the research, involves more than one ethnicity and for this reason the adoption of a word placing the attention on the ethnicity (e.g. *russkij*) is considered inaccurate, while the use of the term "*rossijskij*" is more accurate, since on the one hand it underlines the link with the Russian state, society, culture and language, but on the other it includes other ethnicities, which were present in the former Soviet Union. This aspect is fundamental, because it is exactly from the breakup of the Soviet Union and the conditions characterising the post-Soviet space that emerged the contemporary *Rossijskaja Organizacija*, whose distinctive feature is the multiethnicity. Then, the second term of the terminology proposed, "*Organizacija*", has been preferred by the author from the other terms employed in the literature, namely that one of "*Mafija*". In fact, according to this thesis, the phenomenon of the *Rossijskaja Organizacija* cannot be completely associated with that one of mafia. In particular, the *Rossijskaja Organizacija* lacks the high degree of centralisation and the strict vertical hierarchical structure typical of mafia networks, presenting instead a more horizontal hierarchy and a fluid and flexible nature. Moreover, the relevance given to familial ties and ethnicity in conventional mafia-like networks (e.g. the Italian mafia) are not substantial in shaping the criminal networks belonging to the

Rossijskaja Organizacija. Nevertheless, the *Rossijskaja Organizacija* shares some aspects with mafia-like structures, most notably the fact that it acts as a protection provider, as an alternative to the deficiencies of the State. Moreover, both mafia and the *Rossijskaja Organizacija* strive to acquire power, however, the main objective of the mafia is to control a given territory and to challenge and substitute the State, while the main objective of the *Rossijskaja Organizacija,* at least in Europe, is to make profits without interest to control a specific territory. In fact, the presence of the *Rossijskaja Organizacija* in Europe does not clash with other organised criminal groups active in the same area, instead, a high degree of cooperation with other organised crime groups has been observed. This last aspect has also been underlined in the thesis, by analysing the case study of the *Rossijskaja Organizacija* in Italy, where the Russian criminals do not try to challenge the local mafias, rather they try to find partnerships. Another example that shows the high level of cooperation of the *Rossijskaja Organizacija* with other organised criminal groups is evident in the case of the *Rossijskaja Organizacja* in Germany, where its main features are the poly-criminality and multiethnicity. Therefore, to implement effective countermeasures it is necessary to consider both the composition and the nature of the phenomenon. For instance, a typical approach against mafia-like groups focused on the eradication of the leaders results to be ineffective, since the structure of the branches of the *Rossijskaja Organizacija* is that one of a network with loose and flexible organisation, without a strict hierarchical organisation. Moreover, a typical feature is the high dynamicity in the organisational structure, which adapts itself to the characteristics of the context in which it is operating, as showed by the case of the *Solncevskaja* network, shifting from a hierarchical to a loose affiliation paradigm. Moreover, a number of policy recommendations have been listed to counter the problem of the infiltration of the *Rossijskaja Organizacija* in Europe, such as : the establishment of dedicated units within the police agencies in the EU countries most affected by the phenomenon, on the model of the Russian/Eurasian crime units within the France's *Office centrale de lutte contre le crime organisé (OCLCO)*; the creation in the EU of a cross-departmental body focused on Russian organised crime within Europol, supported by cooperation with the financial intelligence and strategic operations departments; then, the strengthening of the relationships and cooperation with Moscow is required, especially on common areas such as the borders around Kaliningrad and along the border between Finland and Russia; moreover, a higher degree of cooperation among European and Russian investigative agencies, is required.

Concluding remark II: it is fundamental to take into account the cultural, sociological and linguistic dimensions when analysing the *Rossijskaja Organizacija,* in order to understand its strategy and potential targets.

To tackle the problem of the *Rossijskaja Organizacija* is also fundamental to take into account the cultural dimension, which includes knowledge of the historical background as well as of the sociological and linguistic aspects related to the phenomenon. We cannot implement effective countermeasures if we do not know exactly

the object of study taken into consideration. If our goal is to reduce and possibly eradicate the plague represented by the infiltration of the *Rossijskaja Organizacija* in Europe, it is essential to look back at its origin, to consider the starting point in order to understand the evolution, the current outlook and the potential development. For this reason, a whole section of the thesis is dedicated to the historical and cultural aspects, since it is fundamental to understand the group dynamics within the criminal networks as well as the way of thinking and the *modus operandi* employed. For instance, the persistence of old traditions which trace back to the *vory v zakone* (thieves-in-law) of establishing a common fund ('*obščak*'), to which all the members of the criminal community had to pay a contribution or the custom to hold periodic meetings ('*šodka*') with the aim of resolving the conflicts among different clans, nominating the new leaders and defining the criminal strategies. Another example, is represented by the relevance of the prison system and the attention that should be placed by law enforcement authorities over the Russian prisoners, that cannot be fully understood without knowing that the origin of the *Rossijskaja Organizacija* and its culture originated exactly in the prison system during the Stalinist period and that the prison became an headquarter for the Russian criminals. Still nowadays it is in the prisons where the recruitment of new members takes place and where the definition of the roles of each member, the strategies and the alliances are established. Furthermore, another fundamental aspect when considering the *Rossijskaja Organizacija* is the shared past, which is one of the reasons explaining the high level of interdependence and cooperation among different ethnicities belonging to the post-Soviet space and forming different branches of the *Rossijskaja Organizacija*. Furthermore, another element that has been analysed in the thesis is the language, which has a high value in terms of comprehension of the phenomenon. The knowledge of the crypto language employed by the *Rossijskaja Organizacija*, the *fenja* or *ofenskji jasyk*, is in fact an asset to tackle the problem and to implement the necessary countermeasures. As discussed in chapter II, *fenja* traces its origins back to the Middle Ages and underwent substantial transformations throughout the centuries, however it is still spoken by the criminal community and it is still perceived as a threat as demonstrated for example by the law emanated by the Russian Federation in 2013 prohibiting the use of *fenja* in the prisons[351]. The Russian criminal language can be defined a closed system whose main function is secrecy. It is used to classify the different roles of the members of a criminal network, functions, sectors of activities, operations as well as to indicate, with a system of code-names, the different law enforcement authorities. Therefore, knowledge of the *fenja* can also be an asset for the interpretation of the potential targets and operations by means of telephone tapping employed by the law enforcement authorities. Furthermore, another relevant element worth mentioning is the representation of the group within a society, through the set of tools of identification which are sociologically relevant, among which the usage of tattoos in the Russian criminal underworld. Notwithstanding the fact that the contemporary *Rossijskaja Organizacija* is much more integrated into the society of the countries where it operates and that has abandoned high visibility to infiltrate

[351]Gazeta.ru, *Minjust zapretil arestantam materit'cja i «botat' po fene»*, 14th Janyary, 2016. Available at: https://www.gazeta.ru/social/news/2016/01/14/n_8117915.shtml.

the economic and political domains, still it is relevant the discussion of the symbology associated with the criminal tattoos, since they were employed, in the origins, as a representation of the values and believes around which the *vory v zakone* shaped their identity. The criminal tattoos were also a manifestation of the respect or disrespect of the Criminal Code, that has been totally transformed throughout the centuries and whose main provisions, namely the prohibition to collaborate with the authorities, have been totally disregarded. Nevertheless, other provisions relating for instance to the honour code or the mutual assistance to the criminal community are still relevant and respected. Moreover, the representation of a group plays a fundamental role in the comprehension of the group's dynamics and its interaction with the others. The contemporary self-representation of the members belonging to the *Rossijskaja Organizacija* has changed dramatically but it is still of the utmost importance to consider it. The main aim pursued by contemporary Russian criminals is that one of a chameleonic assimilation into the high spheres of the society, the display of a luxury lifestyle, the ambition to acquire more power and ensure to their progeny the best opportunities possible, in order to gain a respected and high position within the society.

Furthermore, from a "cultural" point of view, a set of policy recommendations has been drawn in the present thesis to tackle the problem of the infiltration of the *Rossijskaja Organizacija* in Europe, such as: the need to monitor the Russian expatriate communities in the EU, which must be considered a priority area for security; the requirement for the law enforcement authorities to acquire a better knowledge of those communities, as well as cultivating relationship with them as allies and sources for the intelligence; the assiduous monitoring of the European prisons system should be implemented; the employment of interpreters, by the law enforcement authorities, of the Russian, Ukrainian and Georgian languages with specific knowledge of the criminal crypto language (e.g. *fenja*), thus providing a better knowledge and understanding of the criminal group's strategies and targets.

Concluding remark III: the presence of a "criminal-governmental nexus" in the Russian Federation between the *Rossijskaja Organizacija* and the state apparatus, with consequences on the effects of the phenomenon in Europe.

A relevant assumption discussed in the research is the presence of a "criminal-governmental nexus" in the Russian Federation between the *Rossijskaja Organizacija* and the state apparatus, and the effects of the phenomenon in Europe. A turning point in the relations between organised crime and the Russian state occurred in the 2000s with the raise to the power of Vladimir Putin. Under Putin's presidency the Kremlin has introduced a process of "nationalisation" of the criminal underworld – which emerged as a result of the transition towards the market economy in the aftermath of the collapse of the Soviet Union – with former criminals, which agreed to subordinate to the state power, being enrolled in the top political and economic spheres and, on the other side, the eradication of those in disagreement with the new system introduced by

president Putin. The new mechanism shaping the relations between the Russian state and the criminal business sector is based on the so-called *vertikalnaja sistema* ('vertical system'), which refers to the partial nationalisation of the main industrial sectors, e.g. energy sector, which are of strategic relevance, from which any kind of participation of the so-called oligarchs, that is not controlled and directed by the state, has been excluded. This kind of new relation has also an impact on Europe, specifically in the role played by the Russian security services. There are indeed evidences of the exploitation of the *Rossijskaja Organizacija* abroad by the Russian security apparatus, among which the most striking ones are related to the cyber-attacks directed against Western targets, by means of Advanced Persistent Threat (APT) groups controlled by the Russian intelligence. Particularly, in the thesis a section is devoted to the analysis of the APT28 which is believed to be associated with the Russian military intelligence agency (GRU) and of the APT29, supposedly linked with the Federal Security Service (FSB) and the Foreign Intelligence Service (SVR). Moreover, there are evidences of the recruitment of cybercriminals by the Russian Federation not only to deploy state-controlled operations against Western targets in Europe but also to raise 'black account' funds (*čërnaja kassa*) employed by the Russian state to finance political operations in Europe. Generally, these funds are collected through money laundering activities as discussed in the case presented in the research of the so-called "Russian Laundromat", a sophisticated money laundering scheme executed at detriment of a Western investment company operating in Russia, whose perpetrators included businessmen with strong and even parental ties with the president Putin and the Russian intelligence. Therefore, considering the level of connivance between the Russian state and the *Rossijskaja Organizacija* is fundamental to counter the threat placed by the phenomenon particularly in the legitimate European economy as well as to be aware of the difficulties in the establishment of an effective cooperation with Russian law enforcement authorities, which is required, however, to counter the problem. Nevertheless, we should always take into consideration the framework in which we are moving and be aware of the level of trust which we can expect from our Russian counterparts.

Concluding remark IV: the most relevant threat posed by the *Rossijskaja Organizacija* in Europe is that one deriving from the activities conducted in the legitimate economy, specifically in the financial and banking systems by means of fraud and money laundering schemes.

Furthermore, one of the main sectors to which should be placed the attention and the efforts of the European law enforcement authorities is represented by the financial and banking sectors, where the *Rossijskaja Organizacija* is most active, through the exploitation of sophisticated money laundering schemes and corruption networks within public tenders. Money laundering involves huge amount of capital, which is invested in Europe due to the high standards of privacy and accountability guaranteed by European banks as well as because of the new system introduced by Putin, the so-called *vertikalnaja sistema* ("vertical system"), which reshaped the relationship between the Russian state and the *Rossijskaja Organizacija*, to the benefit of the former. In fact, due to the control exercised by the Kremlin, a considerable amount of capital has been

moved abroad, where it is not subjected to the potential confiscation of the state. As a consequence, more foreign capital, often of unknown or unclear origin, has been invested within European countries, after having been "washed" in countries outside the European Union, where the weaker judiciary and banking systems (e.g. Moldova) allow criminals to launder "black" money. Three case studies have been discussed in the present research to highlight the extension of the phenomenon in object, namely: the "Russian Laundromat", the "Magnitskij affair" and the "Nord Stream case". The first case analysed, the so-called "Russian Laundromat", has been taken into consideration to explain the sophisticated *modus operandi* employed by the *Rossijskaja Organizacija* to launder money as well as to point out the weaknesses of the supervisory system of the European banking system, in which black money are injected after having been "washed" in extra-EU countries; moreover, the case is functional to underline the assumption proposed in the thesis of a "criminal-governmental nexus", which is evident in the case of the "Russian Laundromat", since among the perpetrators of the crime there were individuals with personal or even parental ties with Putin and the Russian political élite. The "criminal-governmental nexus" between the Kremlin and the *Rossijskaja Organizacija* is also discussed in the second case analysed, the "Magnitskij affairs", which is also useful to detect the different steps followed in the implementation of a money laundering mechanism. Then, the third case describes the corruption and money laundering procedures applied by the *Rossijskaja Organizacija* in the realisation of the Nord Stream, a pipeline in the Baltic Sea inaugurated in 2011, developed by Germany and Russia. This case clearly points out the damage and the risk placed by the infiltration of the *Rossijskaja Organizacija* in Europe, as demonstrated by the evidences of corruption and unclear flows of money detected through the analysis of the project. At the European Union level countermeasures have been elaborated to tackle the problem, such as the 5th European Union Anti-Money Laundering Directive (AMLD) adopted in June 2018, representing a turning point for the European Anti-Money Laundering System, as well as the improvement of the Financial Intelligence Units (FIUs). Moreover, a set of policy recommendations has been formulated in this thesis, in order to counter the problem, stressing: the need to focus on the financial and banking systems; the specific attention required on money laundering activities, particularly in the Nordic and Baltic countries; the establishment of an effective mechanism to demonstrate the owners of specific structures and capital invested in the EU as well as the clear origin of the money flows; the implementation of the common European approach against money laundering activity; the stricter supervision over those countries where there have been evidences of major investments made by the *Rossijskaja Organizacija* (e.g. Latvia and Cyprus); the strengthening of the European banking supervisory system, through the imposition of fines to pressure and incentivise continual surveillance by the banks themselves; the request of increased level of transparency and cost estimation related to project management and investments in the EU involving Russian counterparts.

Concluding remark V: the *Rossijskaja Organizacija* is employed as a tool of the Information Warfare (IW) conducted by the Kremlin to pursue its geopolitical agenda and destabilise Europe, in the context of the long-lasting confrontation between the European and Eurasian sides of the continent.

Another fundamental assumption discussed in this thesis is that the *Rossijskaja Organizacija* is exploited by the Kremlin as a tool of the Information Warfare (IW) to pursue its geopolitical agenda and destabilise Europe. In fact, cyberwarfare is included, according to the Russian exegesis, to the wider concept of the *Informacionnaja Vojna* ("Information Warfare"), that is considered in the Russian political and military discourses as a set of methodologies and techniques to acquire power and influence the public opinion as well as a tool at disposal to defend Russia from the West. The literally translation in Russian of the word "cyberwarfare" is '*kibervojna*', however the term is never employed to describe cyberwarfare activities, for which it is rather preferred the expression *Informacionnaja Vojna*. This linguistic choice is not neutral since it involves not only electronic warfare and computer network operations but also psychological operations as well as information and disinformation operations. Thus, cyberwarfare in Russia is considered as part of a wider strategy, developed during the Soviet times, that has changed only in the means employed, while the reasons, tactics and the targets have remained the same. Moreover, from the analysis of the three main interpretations of the IW discussed in the research (the "subversion-war" developed by Messner, the "net-centric war" of Dugin and the "information warfare" elaborated by Panarin), what emerges is the perception, among the Russians, of an on-going confrontation with the West, whose main aim is the manipulation of the informational dimension. Therefore, the cyber domain is considered of the utmost importance both as a defensive and offensive system at disposal to the Russian Federation to defend itself. This ideological framework is fundamental to understand other characteristics of the *Rossijskaja Organizacija*, most notably the degree of connivance with the State, with whom a relation of mutual benefits has been established, based on profits for organised crime in exchange of engagement in activities which have a benefit for the State, such as cyber-attacks directed towards public and private targets belonging to the West.

Concluding remark VI: the cyber domain results to be the most threatened sector by the *Rossijskaja Organizacija,* which is able to take advantage of the technological progress to enhance its activities and to employ the cyber domain as a preferential tool as well as a facilitator for the commitment of crimes.

A relevant assumption has been made about the cybersecurity domain, which is considered in this research as the sector most threatened in Europe by the *Rossijskaja Organizacija*, which benefits of the availability of a well-rooted and high-level scientific expertise in Russia and of the unofficial but substantial support of the State. Given these conditions, the *Rossijskaja Organizacija* has been able to take advantage of the technological progress to enhance its activities and to employ the cyber domain as a preferential tool as well as a facilitator for the commitment of crimes. The tacit support of the Russian state to cybercriminals is evident

in episodes such as the defence of the so-called *patriotičeski chakery* ('patriotic hackers'), as have been defined by Putin those proxy cyber-activists which were supposedly involved in the interference in the 2016 U.S. elections. In fact, as stated in several official documents of the Russian Federation, for the defence of the nation it is reasonable to use unconventional resources (e.g. cybercriminals). The exploitation of cybercriminals to pursue the Russian political agenda is also testified by three cases discussed in the thesis: the DDoS (Distributed Denial-of-Service) attacks against Estonia's internet websites in 2007; the DDoS attacks against Georgia's governmental, economic and communication networks in 2008; the malware attacks against Ukraine in 2013, which were able to open backdoors in the governmental systems and to infiltrate and shut down the power centre networks. However, the most striking example of both the threat placed to the European cybersecurity and the evidence of the support of the Russian state to cybercrime activities is represented by the Advance Persistent Threat (APT) groups APT28 and APT29, which are supposedly controlled by the Russian security services. Specifically, there are evidences, according to which the APT28, whose main targets are government, military and security organisations, is allegedly controlled by the Unit 26165 and Unit 74455 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Russia's military intelligence agency. The other supposedly Russia's controlled group is the APT29, whose main targets are the defence, energy and financial sectors and that is believed to be associated with the Russian Federal Security Services (FSB) and the Foreign Intelligence Service (SVR).

An aspect emerging from the analysis conducted in this thesis is that when the impact of a cyber-attack, allegedly conducted by cybercriminals belonging to the *Rossijskaja Organizacija*, is under consideration, a nexus with a specific geopolitical and military context should be enquired. Moreover, to effectively counter the threat placed by the *Rossijskaja Organizacija* in the cyber domain, we must consider all the variables involved, namely the financial gains as well as the political and geopolitical reasons behind an attack. At the European Union level, a number of measures to counter the problem have been discussed, most notably the EU Cybersecurity Strategy launched for the first time in 2013, the European Agenda on Security 2015-2020, the Directive on Network and Information Security (EU Directive 2016/1148) as well as mechanism such as the Computer Security Incident Response (CSIRT), the Europol's Cybercrime Centre (EC3) and fundamental organisations operating in the cybersecurity domain such as the European Union Agency for Network and Information Security (ENISA). Moreover, specific policy recommendations have been listed, which underline the need to enhance cybersecurity standards for public and private organisations as well as monitoring social networks to detect botnets operations targeting political campaigns or initiatives.

From the analysis conducted in this thesis the threat placed the *Rossijskaja Organizacija* should be placed on the priority agenda of the European Union, due to the increasingly evolving nature of the phenomenon and the high degree of adaptability to the different contexts, as demonstrated in the case studies analysed. Moreover, a specific attention should be placed on the financial and banking systems, specifically in those countries

representing the entry points in the European Union legitimate economy for the *Rossijskaja Organizacija* (e.g. Cyprus, Estonia, Latvia, Lithuania). Furthermore, a trend that has been observed is the increase of the criminal activities conducted in the cyber domain against Western public and private organisations, thus, improvement and further investments in the cybersecurity sector are required. Moreover, due to the specific features of the *Rossijskaja Organizacija* analysed, a fundamental aspect that should not be underestimated in the implementation of an effective approach to counter the threat placed by the phenomenon is constituted by the cultural dimension, involving the knowledge of Russian history, politics and strategic culture, which enable us to be aware of the variables shaping the contemporary outlook of the *Rossijskaja Organizacija* and to provide an interpretation of its distinctive features, tactics and targets. It is only through a deep and complete analysis of the phenomenon, involving the observation of the finest and of apparently not relevant details, that is possible to see the global picture, truly understand the problem and develop the effective measures required to counter it.

REFERENCES

1. Bibliography

Accenture, *Ninth Annual Cost of Cybercrime Study*, 2019. (https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf).

Applebaum Anne, *GULAG. A History*, (Great Britain: The Penguin Press, 2003).

Armao Fabio, *Criminal Clusters: State and Organised Crime in a Globalised World*, The European Review of Organised Crime 1 (1), 2014, 1-44.

Arquilla John and Ronfeldt David, "Cyberwar is coming!", Vol.12 No.2 in *Comparative Strategy*, (Taylor & Francis: 1993), 23-60. (https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf).

Baldev D., Vasiliev S., Sidorov A., *Russian Criminal Tattoo Encyclopaedia*, Vol.3, (London: Fuel Publishing, 2014).

Beck Ulrich, *Risk Society. Towards a New Modernity*, (London: Sage, 1992).

Benvenuti Francesco, *Russia Oggi. Dalla caduta dell'Unione sovietica ai nostri giorni*, (Roma: Carocci editore, 2013).

Braw Elisabeth, *Foreign Fighters Financing*, Foreign Affairs, October 25, 2015.

Bronnikov A., *Russian Criminal Tattoo: Police Files*, Vol.1, (London: Fuel Publishing, 2016).

Bundesamt für Verfassungsschutz, *Cyber Attacks Controlled by Intelligence Services*, 2018. (https://www.verfassungsschutz.de/en/public-relations/publications/publications-cyber-defense/publication-2018-05-cyber-attacks-controlled-by-intelligence-services).

Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2015,* 14th October 2016. (https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html).

Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2016,* 8th August 2017.

(https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html).

Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 1st August 2018. (https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html).

Camera dei Deputati, XVII Legislatura, *Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere*, Seduta n.205, 11th May 2017. (https://www.camera.it/leg17/1058?idLegislatura=17&tipologia=audiz2&sottotipologia=audizione&anno=2017&mese=05&giorno=11&idCommissione=24&numero=0205&file=indice_stenografico).

Caselli Gian Paolo, *La Russia Nuova. Economia e Storia da Gorbačëv a Putin*, (Milano, Udine: Mimesis Edizioni, 2013).

Chang Wei and Wu Jie, *A Survey of Sybil Attacks in Networks*, Department of Computer and Information Sciences Temple University, Philadelphia, 2014. (https://pdfs.semanticscholar.org/97dd/43eabe4789e39b8290cf43daa513483aa4c7.pdf?_ga=2.50091172.327794438.1566547994-1479164381.1566547994).

Cheloukhine Serguei, Maria Haberfeld, *Russian Organized Corruption Networks and their International Trajectories*, (New York, Dordrecht, Heidelberg, London: Springer, 2011).

Chen Peng, Desmet Lieven, Huygens Christophe, "A Study on Advanced Persistent Threats" in De Decker B., Zúquete A. (eds*) Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science*, vol 8735. (Berlin, Heidelberg: Springer, 2014), 63-72. (https://link.springer.com/chapter/10.1007/978-3-662-44885-4_5#citeas).

Choo Kim-Kwang Raymond and Smith Russell G., "Criminal Exploitation of Online Systems by Organised Crime Groups" in Asian Journal of Criminology 3(1):37-59, June 2008, 37-59. (https://www.academia.edu/33267677/Criminal_Exploitation_of_Online_Systems_by_Organised_Crime_Groups).

Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*. (https://clusit.it/rapporto-clusit/).

Connell Michael and Vogler Sarah, Russia's Approach to Cyber Warfare, (Virginia: CNA Analysis & Solutions, March 2017). (https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf).

Corbelli M., *Traducibilità del gergo criminale russo nelle intercettazioni telefoniche in Italia*, (Milano: Fondazione Milano, 2013).

Cornish Paul, Livingstone David, Clemente Dave, Yorke Claire, *On cyber warfare*, (London: The Royal Institute of International Affairs, 2010).
(http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf).

Council of the European Union – General Secretariat of the Council, *Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021 - Council conclusions (18 May 2017)*, Brussels, 19th May 2017.
(http://data.consilium.europa.eu/doc/document/ST-9450-2017-INIT/en/pdf).

Council of the European Union – Standing Committee on Operational Cooperation on Internal Security (COSI), *EU Policy Cycle Terms of Reference*, Brussels, 5th December 2017.
(http://data.consilium.europa.eu/doc/document/ST-10544-2017-REV-2/en/pdf).

De Ficchy Luigi, "La mafia russa ed il fenomeno del riciclaggio transnazionale", Incontro di studio su tema nuove mafie: le organizzazioni criminose straniere operanti in Italia, Consiglio Superiore della Magistratura, Roma, 12-14 Gennaio 2009. pp. 7-12.

Di Nolfo Ennio, *Storia delle relazioni internazionali. Dalla fine della guerra fredda ad oggi*, (Bari: Laterza, 2016).

Dirección General de la Guardia Civil – Jefatura de Información, *Informe sobre la organización criminal euroasiática SOLNTSEVSKAYA. Vínculos con los sujetos investigados. Otras relaciones criminales*, 2016.
(https://tbcarchives.org/tag/solntsevskaya/).

Direzione Investigativa Antimafia (DIA*), Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, Gennaio – Giugno 2018.
(http://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html).

Direzione Investigativa Antimafia (DIA*), Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, Luglio – Dicembre 2018.
(http://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html).

Dugin Aleksandr, *Geopolitika Postmoderna. Vremena novych imperij. Očerki geopolitiki 21 veka* (Sankt-Peterburg: Amfora, 2007).
(https://www.klex.ru/97a).

Dugin Aleksandr, *Russkij Logos – russkij Chaos. Sociologija russkovo obščestva*, (Moskva, Akademičeskij proekt-Gaudamus, 2015).

Dugin Aleksandr, *Sociologija geopolitičeskikh processov Rossii*, (Moskva: Meždunarodnoe «Evrazijskoe Dviženie», 2010).
(https://www.geopolitica.ru/sites/default/files/sgpr-1.pdf).

Dugin Aleksandr, *Vojna kontinentov – sovremennyj mir v geopolitičeskoy sisteme koordinat*, (Moskva: Akademičeskij Proekt, 2015).

EASO, *EU+ asylum trends 2018 overview*, February 2019.
(https://www.easo.europa.eu/sites/default/files/EASO-2018-EU-Asylum-Trends-Overview.pdf).

ENISA, *Threat Landscape Report 2018. 15 Top Cyberthreats and Trends, Final Version 1.0 ETL 2018,* January 2019.
(https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018).

Etter Gregg W., Pottorff Stacia N., Urban Victoria E., *Decoding the Tattoos of the Russian Mafia*, the Journal Gang Research, Vol.25, No.4, August 2018, 1-21.
(https://crimjust.nmsu.edu/files/2019/05/Jounal-of-Gang-Research-Tapia-2018.pdf).

Euipo-Europol, *Intellectual Property Crime Threat Assessment 2019*, 2019.
(https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf).

Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
(https://www.europol.europa.eu/socta/2017/).

Europol, *Europol Programming Document 2019-2021*, adopted by Europol Management Board on 30th November 2018, The Hague, 29th January 2019.
(https://www.europol.europa.eu/publications-documents/europol-programming-document).

Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2018. (https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018).

Europol, *Europol Strategy 2020*, Vienna, 13th December 2018.
(https://www.europol.europa.eu/publications-documents/europol-strategy-2020).

Europol – European Migrant Smuggling Centre (EMSC), *3rd Annual Activity Report 2018*, 2019. (https://www.europol.europa.eu/publications-documents/emsc-3rd-annual-activity-report-%E2%80%93-2018).

European Banking Authority, *Final Guidelines on Risk Factors*, JC 2017 37, 26th June 2017. (https://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf).

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security*, Strasbourg, 28th April 2015.
(https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf).

European Commission – Directorate-General for Education, Youth, Sport and Culture, *Illicit trade in cultural goods in Europe. Characteristics, criminal justice responses and an analysis of the applicability of technologies in the combat against the trade*, (Luxembourg: Publications Office of the European Union, 2019).
(https://publications.europa.eu/en/publication-detail/-/publication/d79a105a-a6aa-11e9-9d01-01aa75ed71a1).

European Commission, *European agenda on migration*, Brussels, 2015.
(https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-migration_en).

European Commission, *EU Data collection on trafficking in human beings in the EU*, Brussels, 2018. (https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181204_data-collection-study.pdf).

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *European Drug Report 2018: Trends and Developments*, June 2018.
(http://www.emcdda.europa.eu/publications/edr/trends-developments/2018).

European Union Action to Fight Environmental Crime, *Environmental Crime and the Eu Synthesis of the Research Project "European Union Action to Fight Environmental Crime" (Efface)*, (Berlin: Ecologic Institute gGmbH, March 2016).
(https://www.ecologic.eu/sites/files/publication/2016/efface_synthesis-report_final_online.pdf).

Feodorov S.G., "Obyčnoe pravo, samosud i konokradstvo v rossijskoj i sibirskoj derevnjach vo vtoroj polovine XIX veka", in *Gumanitarnye Nauki*, Vypusk 9, Vestnik Kurganskovo gosudarstvennogo universiteta, 2013.

Fijnaut Cyrille and Paoli Letizia, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004).

Fijnaut Cyrille, Paoli Letizia (eds) *Organised Crime in Europe*. Studies of Organized Crime, Vol. 4, (Dordrecht: Springer, 2004).

Finckenauer James O., Voronin Yuri A., *The Threat of Russian Organized Crime*, Issues in International Crime, NCJ 187085, June 2001.

Finckenauer James O., Waring Elin J., *Challenging the Russian Mafia Mystique*, National Institute of Justice Journal, April 2001.

Finckenauer James O. and Waring Elin J, *Russian Mafia in America: Immigration, Culture, and Crime*, (Boston: Northeastern University Press, 1998).

Freeland Chrystia, *Sale of the century: Russia's wild ride from communism to capitalism*, (New York: Crown Publishers, 2000).

FRONTEX, *Risk Analysis for 2018*, Warsaw, 2018. (https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_for_2018.pdf).

Galeotti Mark, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*, European Council of Foreign Relations, April 2017.

Galeotti Mark, *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations, May 2016.

Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Heaven and London: Yale University Press, 2018).

Gambetta Diego, *The Sicilian Mafia. The Business of Private Protection*, (Harvard: Harvard University Press, 1993).

Ghafir Ibragim and Prenosil Vaclav, *Advance Persistent Threat Attack Detection: An Overview*, International Journal of Advancements in Computer Networks and Its Security – IJCNS, Vol.: Issue 4 [ISSN 2250-3757], 2014.
(https://www.researchgate.net/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview).

Gilinskiy Yakov and Kostjukovsky, "From Thievish *Artel* to Criminal Corporation: The History of Organised Crime in Russia" in Fijnaut Cyrille and Paoli Letizia, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004). pp. 189-191.

Giustozzi Corrado, *Commentary: Cybercrime as a service*, Istituto per gli studi di politica internazionale (ISPI), July 2018.
(https://www.ispionline.it/en/pubblicazione/cybercrime-service-20979).

Gološčapova T.G., Mirmovič T.D., *Naimenovanija Lica v Kriminal'nom Mire*, Vikitimologija 1(7), 2016.

Gračev M.A., *Blatnaja Muzyka*, Journal «Musart» №3, vesna 2006.

Gračev M.A, Mokienko V.M., *Russkij žargon. Istoriko-étimologičeskij slovar'*, (Moskva: AST-Press, 2009).

Graziosi Andrea, *L'URSS di Lenin e Stalin. Storia dell'Unione Sovietica 1914-1945*, (Bologna: Il Mulino, 2007).

Graven J., *L'argot et le tatouage des criminels*, (Neuchâtel: Histoire et Société d'aujourd'hui – Editions de la Bconnière, 1962.

Gutauskas Aurelijus, "Lithuania" in Kegö Walter, Molcean Alexandru (Ed.), *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, (Stockholm-Nacka: Institute for Security and Development Policy, 2012), 78-87.

Halbwachs Maurice, *On Collective Memory*, edited and translated by Lewis A. Coser, (Chicago and London: The University of Chicago Press, 1992).

International Telecommunication Union (ITU), *Overview of cyber security, ITU-T X-Series Recommendations Data Networks, Open System Communications and Security*, Rec. ITU-T X.1205 (04/2008).
(https://www.itu.int/rec/T-REC-X.1205-200804-I).

Jaitner Margarita, “Russian Information Warfare: Lessons from Ukraine”, Chapter 10 in Kenneth Geers (eds.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications, 2015).
(https://www.academia.edu/24846469/Russian_Information_Warfare_Lessons_from_Ukraine).

Juurvee Ivo, *The resurrection of ‘active measures’: Intelligence services as a part of Russia’s influencing toolbox*, Strategic Analysis, April 2018.

Kadlecová Lucie, *Russian-speaking Cyber Crime: Reasons behind its Success*, (The European Review of Organised Crime, 2015).
(https://www.academia.edu/16548880/Russianspeaking_Cyber_Crime_Reasons_behind_Its_Success).

Karpanos Ilona, *The Political Economy of Organised Crime in Russia: The State, Market and Criminality in The Ussr and Post-Soviet Russi*a, (London: Department of International Politics, 2017).

Keene Shima D., *Silent Partners: Organized Crime, Irregular Groups, and Nation-States*, Strategic Studies Institute and U.S. Army War College Press, U.S., October 2018.

Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011).

Kegö Walter, Georgieff Alexander, *The Threat of Russian Criminal Money: Reassessing EU Anti-Money Laundering Policy*, (Stockholm: Institute for Security and Development Policy, 2013).

Kirschenbaum Joshua, Tofilat Sergiu, *Massive Russian Financial Flows Through Moldova Show Small Jurisdiction Matter*, The German Marshall Fund of the United States, 26th July 2019. (www.gmfus.org/sites/default/files/Massive%20Russian%20Financial%20Flows%20Through%20Moldova%20Show%20Small%20Jurisdictions%20Matter.pdf).

Kojevnikov Alexei, *The Phenomenon of Soviet Science*, (Vancouver: The History of Science Society, 2008).
(https://pdfs.semanticscholar.org/ccb5/3de6cda73022bfa0b2358899b76a3f82f8a4.pdf).

Koskensalo A., *Secret Language Use of Criminals: Their Implications to Legislative Institutions, Police, and Social Policies*, Sino-US English Teaching, Vol.12, No. 7, July 2015.

Kramer Franklin D., Starr Stuart H. and Wentz Larry K., *Cyberpower and National Security*, (Washington:National Defense University Press, 2009).

Krivova N.F., *Kategorija social'noj ocenki v gruppe suščestvitel'nych so značeniem lica,* Lingvistika Vestnik Nižegorodskovo universiteta N.M. Lobačevskogo ,2010, № 4 (2), c. 572–574.

Krylosova S., *Les particularités d'emploi des mots argotiques en russe contemporain*, Cahiers du DNPS : Linguistique et politique, 2003.

Lichačev D.S., "Argotičeskie slova professional'noj reči" in *Razvitie grammatiki i leksiki sovremmenogo russkogo jazyka*, Moskva, 1964, 311-359.

Lill Liis, "Estonia" in Kegö Walter, Molcean Alexandru (Eds.), *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, (Stockholm-Nacka: Institute for Security and Development Policy, 2012), 54-66.

Loskutovs Aleksejs, *Transnational Organised Crime – Latvian Challenges and Responses*, Connections QJ, No. 3, 2016.

Lumans Valdis O., *Latvia in World War II*, (New York: Fordham University Press, 2006).

Lusthaus Jonathan, *Industry of Anonimity: Inside the Business of Cybercrime*, (Cambridge: Harvard University Press, 2018).

Makarenko Tamara, *The Crime–Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism*, Global Crime, Vol. 6, No. 1, February 2004, 129-145.
(https://www.iracm.com/wp-content/uploads/2013/01/makarenko-global-crime-5399.pdf).

Mars Gerald, Altman Yochanan, *The cultural bases of soviet Georgia's second economy*, Journal of Soviet Studies, Volume 35, Issue 4, 1983, 546-560.

Messner Evgeny, "Imja Tret'ej Vseminoj" in *Vsemirnaja mjateževojna*, (Moscow: Kuchkovo Pole, 2004).

Messner Evgeny, "Lik sovremennoj vojny", Volume 2 *of Problemy vojny i mira*, (Južno-Amerikanskij otdel Instituta po issledovaniju problem vojny i mira im. Generala prof. N.N. Golovina, 1959).

Michaeljan M.E., *Some Pragmalinguistic Peculiarities of Criminal and Pseudo-Criminal Types of Discourse*, (Pjatigorsk: Pjatigorskij Gosudarstvennyj Lingvističeskij Universitet, 2017).

Mokienko V.M., Nikitina T.G., *Slovar' Žargona – Bol'šoj Slovar' Russkovo Žargona*, SPB, 2000.

Mullins Sam and Wither James K, *Terrorism and Organized Crime*, Connections: The Quarterly Journal, No.3, 2016.
(https://www.jstor.org/stable/pdf/26326452.pdf?refreqid=excelsior%3A63ce683f2047287642301f98c5aaba02).

Mwiki Henry, Dargahi Tooska, Dehghantanha Ali, and Choo Kim-Kwang Raymond Choo, *Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin*, (Switzerland: Springer, 2019).
(https://www.researchgate.net/publication/330071595_Analysis_and_Triage_of_Advanced_Hacking_Groups_Targeting_Western_Countries_Critical_National_Infrastructure_APT28_RED_October_and_Regin_Theories_Methods_Tools_and_Technologies/link/5ca3d8af458515f7851fcf4a/download).

Nikonov Vyacheslav, "Russkij Mir: Smysly i Cennosti" Ch.3 in *Smysly i Cennocti Russkovo Mira. Sbornik statej i materialov kruglych stolov, organizovannych fondom «Russkij mir»*, (Moskva: Fond Russkij Mir, 2010).

NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*. Special Publication 800-39, 2010.
(https://www.nist.gov/publications/managing-information-security-risk-organization-mission-and-information-system-view).

Nurse Jason R. and Bada Maria, "The Group Element of Cybercrime: Types, Dynamics, and Criminal Operation" in *The Oxford Handbook of Cyberpsychology*, edited by Alison Attrill-Smith, Chris Fullwood, Melanie Keep, and Daria J. Kuss, (Oxford: 2018).
(https://www.researchgate.net/publication/328763267_The_Group_Element_of_Cybercrime_Types_Dynamics_and_Criminal_Operations).

Olenik A., *Un double monstrueux: la culture criminelle en Russie post-sovietique*, Cultures & Conflicts 42, June 2001.

Ortner Daniel, *Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime*, BYU L. Rev. 177, 2015.
(https://digitalcommons.law.byu.edu/lawreview/vol2015/iss1/7).

Panarin Igor, *Informacionnaja Vojna I kommunikacii*, (Moscow: Goryachaya Liniya-Telekom, 2015).

Pasko Grigory, "Non-transparent and dubious actions during the construction of the Nord Stream gas pipeline" in *Russian "Black Money" in the EU: Indicators of Transborder Corruption*, EU-Russia Civil Society Forum, December 2015.

Pawar Mohandas and Anuradha J., *Network Security and Types of Attacks in Network*, Conference Paper in Procedia Computer Science, May 2015.
(https://www.semanticscholar.org/paper/Network-Security-and-Types-of-Attacks-in-Network-Pawar-Anuradha/2e03854bc7712720dfd6f9c2d8cb9f10082d88bd).

Pfetsch Barbara, *"In Russia we were Germans, and now we are Russians." Dilemmas of Identity Formation and Communication among German-Russian Aussiedler*, (Berlin: Science Center Berlin for Social Research, 1999).

Ponemon Institute LLC and Accenture, *The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study. Unlocking the Value of Improved Cybersecurity Protection*, 2019.
(https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf).

Popescu Nicu and Secrieru Stanislav, *Hacks, Leaks and Disruptions. Russian Cyber Strategies*, (Paris: Chaillot Papers, European Union Institute for Security Studies, 2018).
(https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf).

Presidential Decree No. 537, *Russia's National Security Strategy to 2020*, 12nd May 2009.
(Available in Russian at http://kremlin.ru/supplement/424 and available in English at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020).

Presidential Decree No. 646, *Doctrine of Information Security of the Russian Federation*, Moscow, 5th December 2016.
(Available in Russian at https://info.publicintelligence.net/RU-InformationSecurity-2016.pdf and in English at http://afyonluoglu.org/PublicWebFiles/strategies/Asia/Russia%202016%20Information%20Security%20Doctrine.pdf).

Presidential Decree No. 683, On the Russian Federation National Security Strategy, Moscow, 31 December 2015.
(Available in Russian at https://xn--b1aew.xn--p1ai/upload/site1/document_file/Ukaz_683-2015_d1(4).pdf and in English at http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf).

Presidential Decree No. 1753, *Osnovy gosudarstvennoj politiki Rossijskoj Federacii v oblasti meždunarodnoj informacionnoj na period do 2020*, 24th June 2013.
(http://www.scrf.gov.ru/security/information/document114/).

Presidential Decree No. 2976, *The Military Doctrine of the Russian Federation*, 25th December 2014. (Available in Russian at https://rg.ru/2014/12/30/doktrina-dok.html and available in English at https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf).

Presidenza del Consiglio dei Ministri - Sistema di Informazione per la Sicurezza della Repubblica, *Documento di Sicurezza Nazionale*, 2018.
(http://www.sicurezzanazionale.gov.it/sisr.nsf/Relazione-2018.pdf).

PricewaterhouseCoopers, *Russian Economic Crime and Fraud Survey 2018. Combating Fraud: measures taken by companies*, 2019.
(https://www.pwc.ru/en/forensic-services/assets/PwC-RECS-2018-eng.pdf).

Reitano Tuesday, Clarke Colin, Adal Laura, *Examining the Nexus between Organised Crime and Terrorism and its implications for EU Programming*, CT MORSE – Counterterrorism, Monitoring, Reporting and Support Mechanism, 2017.
(https://icct.nl/publication/examining-the-nexus-between-organised-crime-and-terrorism-and-its-implications-for-eu-programming/).

Reuter Peter, *The organization of illegal markets: An economic analysis*, (Washington: U.S. National Institute of Justice, 1985).

Riasanovskij Nicholas V., *Storia della Russia. Dalle origini ai giorni nostri*, (Milano: Bompiani/Rizzoli Libri S.p.A., 1989/2016).

Roberts James Q., *Maskirovka 2.0: Hybrid Threat, Hybrid Response*, (Florida: Joint Special Operations University Center for Special Operations Studies and Research, December 2015).
(https://apps.dtic.mil/dtic/tr/fulltext/u2/1007494.pdf).

Savona Ernesto U. and Mancuso Marina (eds.). 2017. *Fighting lllicit Firearms Trafficking Routes and Actors at European Level. Final Report of Project FIRE*, (Milano: Transcrime – Università Cattolica del Sacro Cuore, 2017).
(www.fireproject.eu).

Savona Ernesto U. and Riccardi Michele (Eds.), *From illegal markets to legitimate businesses: the portfolio of organised crime in Europe*, (Trento: Transcrime – Università degli studi di Trento, 2015).

Savona Ernesto U. and Riccardi Michele (Eds), *Mapping the risk of Serious and Organised Crime infiltration in European Businesses – Final report of the MORE Project*, (Milano: Transcrime – Università Cattolica del Sacro Cuore, 2018).

Shelley Louise, "Contemporary Russian Organised Crime: Embedded in Russian Society" in Fijinaut and Paoli, *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dordrecht, The Netherlands: Springer, 2004), 563-584.

Shelley Louise, "Georgian organized crime" in Shelley Louise, Scott Erik R. and Latta Anthony (Ed.), *Organized Crime and Corruption in Georgia*, (London and New York: Routledge, 2007). 61-68.

Siegel Dina, *Lithuanian itinerant gangs in the Netherlands*, Kriminologijos Studijos, No.2 2014.

Simcox Robin, *'We Will Conquer Your Rome': A Study of Islamic State Terror Plots in the West*, The Henry Jackson Society, Center for the Response to Radicalisation and Terrorism (CRT), 2015.

Slade Gavin, *Mafia and Anti-Mafia in the Republic of Georgia: Criminal Resilience and Adaptation Since the Collapse of Communism*, (Oxford: St. Antony's College, 2011).

Smith David J., *How Russia Harnesses Cyberwarfare*, Defense Dossier, Issue 4, August 2012.

Strods Heinrihs, "Sovietization of Latvia 1944–1991" Nollendorfs Valters, Oberländer Erwin (Ed.), *The Hidden and Forbidden History of Latvia under Soviet and Nazi Occupations 1940-1991*, (Riga: Institute of the History of Latvia, 2005), 209-227.

Sukharenko Alexander N., *Russian ITC Security Policy and Cybercrime*, PONARIS Eurasia Policy Memo No.601, July 2019.
(http://www.ponarseurasia.org/memo/russian-itc-security-policy-and-cybercrime).

Svetlana Alexievitch, *Vremia second hand (konec krasnovo čeloveka)*, (Moskva, Vremia, 2013).

Swisscom Ltd Group Security, *Cyber Security Report 2019*, (Switzerland: February 2019). (https://www.swisscom.ch/content/dam/swisscom/en/about/company/portrait/network/security/documents/security-report-2019.pdf.res/security-report-2019.pdf).

The Swiss Federal Office of Police – Service for Analysis and Prevention, *Strategic Analysis Report: Organised Crime and the Special Services of the Commonwealth of Independent States*, June 2007. (https://tbcarchives.org/fsb-and-organized-crime-connection-analytical-report/).

Timroth V.W., *Russian and Soviet Sociolinguistics and Taboo Varieties of the Russian Language (Argot, Jargon, Slang and "Mat")*, (München, Verlag Otto Sagner, 1986).

Transparency International Latvia (Sabiedriba par atklatibu – Delna), *Connections. Money laundering in Latvia and the role of trust and company service providers*, January 2018.

TrendMicro and U.S. Secret Service Criminal Investigation Division (CID), *The Evolution of Cybercrime and Cyberdefense*, 2018.
(https://documents.trendmicro.com/assets/white_papers/wp-evolution-of-cybercrime-and-cyberdefense.pdf).

Ugolovnyj kodeks Rossijskoj Federeacii,1996.
(Available in Russian at http://ukodeksrf.ru/skachat-uk-rf and available in English at https://www.legislationline.org/documents/section/criminal-codes/country/7/Russian%20Federation/show).

UNESCO, *The Protection of Heritage and Cultural Diversity: a Humanitarian and Security Imperative in the Conflicts of the 21st century*, Background note to the International Conference "Heritage and Cultural Diversity at Risk in Iraq and Syria", Paris, December 2014. (https://en.unesco.org/system/files/iraqsyriaeventbackgroundnoteeng.pdf).

United Nations – General Assembly, *United Nations Convention on Transnational Organized Crime (UNTOC)*, RES. 55/25, 15th November 2000.
(https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf).

United Nations, International Narcotics Control Board, *Report 2017*, January 2018. (https://www.incb.org/documents/Publications/AnnualReports/AR2017/Annual_Report/E_2017_AR_ebook.pdf).

United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, (New York: United Nations, 2013). (https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf).

United Nations Office on Drugs and Crime (UNODC), *Drug Money: the illicit proceeds of opiates trafficked on the Balkan route*, 2015.
(https://www.unodc.org/documents/data-and-analysis/Studies/IFF_report_2015_final_web.pdf).

United Nations Office on Drugs and Crime (UNODC), *Global Study on Smuggling of Migrants 2018*, June 2018.
(https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf).

United Nations Office on Drugs and Crime (UNODC), *Results of a pilot survey of forty selected organized criminal groups in sixteen countries*, September 2002.
(https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf).

United Nations Office on Drugs and Crime (UNODC), *The Globalization of Crime. A transnational Organized Crime Threat Assessment*, 2010. (https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf).

United Nations Office on Drugs and Crime (UNODC), *World Drug Report*, 2018.
(https://www.unodc.org/wdr2018/).

Varese Federico, *Mafias on the Move. How Organized Crime Conquers New Territories*, (Princeton, Oxford: Princeton University Press, 2011).

Varese Federico, *The Russian Mafia. Private Protection in a New Market Economy*, (Oxford: Oxford University Press, 2005).

Varese Federico, "What is Organized Crime?" in F. Varese (ed.), *Organized Crime: Critical Concepts in Criminology*, (London: Routledge, 2010).

Vilks Andrejs, "Latvia" in Kegö Walter, Molcean Alexandru (Ed.), *Russian Organized Crime: Recent Trends in the Baltic Sea Region*, (Stockholm-Nacka: Institute for Security and Development Policy, 2012), 67-77.

Volkov Vadim, "The Russian Mafia: Rise and Extinction", Ch.7 in *The Ofxord Handbook of Organized Crime*, edited by Letizia Paoli, (Oxford, New York: Oxford University Press, 2014).

Von Humboldt Wilhelm, "Latium und Hellas oder Betrachtungen über das classische Alterthum", in *Ausgewählte Schriften* (Berlin: Zenodot Verlagsgesellschaft mbH, 2014).

Wieclawski Jacek, *The Case of the Russians in Latvia and the Need of the Comprehensive Research Approach in Contemporary International Relations*, Institute of Political Science, University of Warmia and Mazury in Olsztyn, Poland, February 19, 2015.

Williams Paul D. and McDonald Matt, *Security Studies. An Introduction*, 3rd ed., (New York: Routledge, 2018).

Wirtz James J., "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy", Chapter 3 in Kenneth Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, (Tallinn: NATO CCD COE Publications, 2015). (https://ccdcoe.org/uploads/2018/10/Ch03_CyberWarinPerspective_Wirtz.pdf).

Zornickij A.V., *Evrejskie Ètimologii Russkich Ugolovnych Argotizmov i Metodologičeskie Trudnosti ich Izučenija*, Novitnja filologija (41), 2012, pp. 63-79.

Zugumov Z.M., *Russkojazyčnyj žargon. Istoriko-étimologičeskij tolkovyj slovar' prestupnovo mira*, (Moskava: Knižnym mir, 2015).

2. Sitography

BBC-Russkaja Služba, *Putin: khakerami možet dvigat' patriotičeskij nastroj*, June 2017. (https://www.bbc.com/russian/news-40118501).

Bundesamt für Migration und Flüchtlinge – Bamf, *Statiskitken*, 2018. (http://www.bamf.de/DE/Infothek/Statistiken/statistiken-node.html).

C-net, *Russian police: 'Our hackers are the best'*, 11th April 2005. (https://www.cnet.com/news/russian-police-our-hackers-are-the-best/).

Centrālās statistikas pārvaldes datubāzes, *Latvija*, 2018. (https://data.csb.gov.lv/pxweb/lv/iedz/iedz__iedzrakst/IRG080.px/?rxid=cd00d9dc-a4e4-4b85-a975-e8b416dee23e.)

Council on Foreign Relations, *Cyber Operation Tracker*, 2019. (https://www.cfr.org/interactive/cyber-operations/apt-28).

Eesti Statistika, *Rahvaarv rahvuse järgi*, 1. Jaanuar, aasta, 6th June 2019.
(https://www.stat.ee/34267).

Europol, *Online Sale of Fake Medicines and Products Targeted in Operation Pangea IX*, Press Release, 2016.
(https://www.europol.europa.eu/newsroom/news/online-sale-of-fake-medicines-and-products-targeted-in-operation-pangea-ix).

Europol, *Operation Takes Down Over 33 600 Internet Domains Selling Counterfeits Goods*, Press Release, 2018.
(https://www.europol.europa.eu/newsroom/news/operation-takes-down-over-33-600-internet-domains-selling-counterfeits-goods).

Europol – Press Release, *Darknet Arms Vendor Arrested in Slovenia with Support of Europol*, 20th December 2016.
(https://www.europol.europa.eu/newsroom/news/darknet-arms-vendor-arrested-in-solvenia-support-of-europol).

European Commission, *Combating Environmental Crime*, 7th August 2019.
(https://ec.europa.eu/environment/legal/crime/).

European Commission, *European Commission welcomes the Council adoption of visa liberalisation for the citizens of Ukraine*, Brussels, 11th May 2017.
(https://europa.eu/rapid/press-release_STATEMENT-17-1270_en.htm).

European Commission – Press Release, *Fight against money laundering and terrorist financing: Commission assesses risks and calls for better implementation of the rules*, Brussels, 24th July 2019.
(https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4452).

European Union Agency for Cybersecurity, *Botnets*, 2019.
(https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets).

Financial Action Task Force on Money Laundering (FATF), *What is Money Laundering?*, 2019.
(https://www.fatf-gafi.org/faq/moneylaundering/).

FireEye Threat Intelligence, *APT28: A Window into Russia's Cyber Espionage Operations?*, 2014.
(https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf).

FireEye Threat Intelligence, *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, 2015.
(https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html).

Forcepoint, *What is Malware? Malware Defined, Explained, and Explored*, 2019.
(https://www.forcepoint.com/cyber-edu/malware).

Forcepoint, *What is Spoofing? Spoofing Defined, Explained, and Explored*, 2019.
(https://www.forcepoint.com/cyber-edu/spoofing).

Gazeta.ru, *Minjust zapretil arestantam materit'cja i «botat' po fene»*, 14th Janyary, 2016.
(https://www.gazeta.ru/social/news/2016/01/14/n_8117915.shtml).

Gazprom, *Gas Pipeline: Nord Stream. The gas pipeline directly connecting Russia and Europe*, 2012.
(https://www.gazprom.com/projects/nord-stream/).

Gazprom, *Gas Pipeline: Nord Stream 2. A new export gas pipeline running from Russia to Europe across the Baltic Sea*, 2018.
(https://www.gazprom.com/projects/nord-stream2/).

Grigas Agnia, Trakimavičius Lukas, *Nord Stream 2 is a Bad Deal for Europe*, Atlantic Council, 10th July 2018.
(https://www.atlanticcouncil.org/blogs/new-atlanticist/nord-stream-2-is-a-bad-deal-for-europe).

Hjelmgaard Kim, *European Welfare Benefits Help Fund ISIS Fighters*, USA Today, February 23, 2017.
(https://eu.usatoday.com/story/news/world/2017/02/23/european-welfare-benefits-fund-islamic-state-isis-fighters/98290438/)

Italian National Institute of Statistics (ISTAT), *Demographic data*, 2019.
(http://dati.istat.it/Index.aspx).

Kaspersky, *What Is a Data Breach?*, 2019.
(https://www.kaspersky.com/resource-center/definitions/data-breach).

Kaspersky, *What is a DDoS Attack? - DDoS Meaning*, 2019.
(https://www.kaspersky.com/resource-center/threats/ddos-attacks).

Lehberger Roman, *BKA warnt vor Tschetschenen-Mafia*, Der Spiegel, 09.05.2019.
(https://www.spiegel.de/panorama/justiz/bka-warnt-vor-tschetschenen-mafia-a-1266338.html).

L'Espresso, *I trafficanti di uomini che Matteo Salvini non vuole vedere vengono dalla Russia*, 12th April 2019.
(http://espresso.repubblica.it/plus/articoli/2019/04/11/news/i-trafficanti-di-uomini-che-salvini-non-vedescafisti-russi-1.333644).

L'Espresso, *Inchiesta: Così i signori dei furti venuti dall'Est la fanno sempre franca (Ultime vittime? I Salvini)*, 30th August 2018.
(http://espresso.repubblica.it/inchieste/2018/08/30/news/cosi-i-signori-dei-furti-est-la-fanno-franca-vittime-salvini-1.326377).

Malwarebytes, *The New Mafia: Gangs and Vigliantes. A Guide to Cybercrime for CEOs*, 2017. (https://www.malwarebytes.com/pdf/white-papers/Cybercrime_NewMafia.pdf).

Ministry of Defence of the Russian Federation, *Konceptual'nye vzgljady na dejatel'nost' Vooružennych Sil Rossijskoj Federacii v informacionnom prostranstve*. (http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle).

Official Internet Resources of the President of Russia, *Speech at the Meeting of Russian Federation ambassadors and permanent envoys in Moscow*, 30 June 2016. (http://en.kremlin.ru/events/president/news/52298).

Organised Crime and Corruption Reporting Project (OCCRP), *Spain: Russian Kemerovskaya Gang Leader Arrested in Joint Spanish-Estonian Operation*, 8th August 2017. (https://www.occrp.org/en/component/content/article?id=6829:spain-russian-kemerovskaya-gang-leader-arrested-in-joint-spanish-estonian-operation).

Organised Crime and Corruption Reporting Project (OCCRP), *The Russian Laundromat*, 22nd August 2014. (https://www.reportingproject.net/therussianlaundromat/russian-laundromat.php).

Paloalto networks, *What Is a Denial of Service Attack (Dos)? An Overview of Dos Attacks*, 2019. (https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos).

Prestupnaja Rossija – Organizovannaja Prestupnost', *V Éstonii načinaetsja sud nad liderami «Kemerovskoj» OPG*, 21st January 2018. (https://crimerussia.com/organizedcrime/v-estonii-nachinaetsya-sud-nad-liderami-kemerovskoy-opg/).

Schengen VisaInfo, *Georgian citizens can travel to the Schengen Zone without a visa*, 27th March 2017. (https://www.schengenvisainfo.com/news/georgian-citizens-can-travel-to-the-schengen-zone-without-a-visa/).

Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (TAX3), *Public Hearing: "Money Laundering Cases Involving Russian Individuals and their effect on the EU"*, 29th January 2019. (Transcription (verbatim) available at: http://www.europarl.europa.eu/cmsdata/161080/CRE_TAX3_20190129.pdf).

Symantec, *APT28: New Espionage Operations Target Military and Government Organizations*, October 2018. (https://www.symantec.com/blogs/election-security/apt28-espionage-military-government).

TechRepublic, *Profiling and categorizing cybercriminals*, 2010.

(http://www.techrepublic.com/blog/security/profiling-and-categorizing-cybercriminals/4069).

Telegraf.rs, *Ruska mafija važi za najopasniju na svetu: Vlada surovim metodama, ima 300.000 članova, a njihove veze sa državom su veoma moćne*, 9th October 2017.
(https://www.telegraf.rs/zanimljivosti/svastara/2902316-ruska-mafija-vazi-za-najopasniju-na-svetu-vlada-surovim-metodama-ima-300000-clanova-a-njihove-veze-sa-drzavom-su-veoma-mocne).

Transborder Corruption Archive, Dirección General de la Guardia Civil – *Jefatura de Información*, *Anális parcial contenido teléfono de un investigato*, 2018.
(https://tbcarchives.org/tag/solntsevskaya/).

Vedmosti, *Top-menedžera «dočki» «Rostecha» zaderžali v Italii po zaprosu SŠA. Ego podozrevajut v èkonomičeskom špionaže*, 05 September 2019.
(https://www.vedomosti.ru/politics/articles/2019/09/05/810548-zaderzhali-italii?fbclid=IwAR2mc-jDiDWLrtfxbmL2Qwfd5m-ol93iWNfmzFdT23zye-8-VfUs1ErzrDY).

SUMMARY

The aim of this thesis is to highlight the nature and extent of the threat placed by organised crime to the European security architecture, specifically through the analysis of the Russian organised crime in Europe, for whom the expression *Rossijskaja Organizacija* has been proposed in the present research. The main hypothesis formulated is that organised crime in general and specifically the *Rossijskaja Organizacija* can be considered a distorted form of governance, affecting not only security in strict terms but the economy and society as a whole. The current model to which organised crime can be ascribed is that one of a complete *mimesis* of the ordinary structures of the society and of a profound infiltration into the economic and political domains, which in some cases evolve into a cohabitation paradigm, characterised by the creation of grey zones, where the line between illicit and licit operations becomes blurred. In the research, both the activities carried out by organised crime in the illegal and legal markets are taken into consideration, however, the key assumption is that the most challenging threat for the European security is represented by criminal operations conducted within the boundaries of the legitimate economy. Moreover, to demonstrate the relevance of the activities conducted within the European legal market by organised crime groups, the case study of the infiltration of *Rossijskaja Organizacija* in Europe has been extensively analysed, on the basis of the key hypotheses formulated in the thesis, according to which there is a "criminal-governmental nexus" between the *Rossijskaja Organizacija* and the Russian state, that exploits the Russian criminal networks in Europe as a tool to pursue its geopolitical agenda and as a mean at disposal for the *Informacionnaja Vojna* ('Information Warfare') against the West, in the context of the struggle between the European and Eurasian models for hegemony, particularly evident in the analysis conducted on the Russian threat to the European cybersecurity system.

I. In the first chapter, the characteristics of organised crime in Europe are presented as well as the main activities carried out and the profits thereof. According to Europol, there are more than 5.000 international organised crime groups (OCGs) currently under investigation in the European Union (EU), belonging to more than 180 nationalities[352]. The main features showed by OCGs in Europe are the poly-criminality, with 45% of them operating in more than three countries, and the ability to take advantage of the technological progress. Furthermore, a trend observed in contemporary organised crime is the increasingly growth of the involvement in the European legitimate economy, where evidences of laundering of illicit proceeds have been detected. In fact, investments in the legitimate economy act as facilitators for the deployment of illicit activities, employing for instance covered companies as "legitimate" frontline actors of illicit trafficking (e.g. transport and shipping companies) and for executing fraud schemes and money laundering operations (e.g. shell companies and insurance frauds). Moreover, another relevant element analysed is the threat emerging form the nexus between organised crime and terrorism, the latter being financed by OCGs, that is also exploited by terrorists to obtain

[352] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017. Available at: https://www.europol.europa.eu/socta/2017/.

firearms or counterfeited documents and to let operatives enter into the European Union (EU) through migrant smuggling activities.

Considering the European illicit market, it generates approximately €110 billion euros each year[353] and includes different criminal sectors, among which the most relevant are drug trafficking, migrant smuggling, trafficking in human beings, illegal trafficking of firearms, cyber-dependent crimes, economic crime, property and environmental crimes.

The illegal production and trafficking of narcotics is one of the main threats to the European security. It is estimated that in the EU the illicit drug market generates about €24 billion euros per year[354], thus being one of the most lucrative criminal activities in the EU, accounting for more than one third of the OCGs operations. According to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) the largest profit of the EU illicit drug market shares comes from the cannabis (€9.3 billion euros), followed by heroin (€6.8 billion euros), cocaine (€5.7 billion euros), amphetamines (€1.8 billion euros) and ecstasy (€0.7 billion euros)[355].

Another relevant sector within the illegal market is represented by migrant smuggling, which generates profits comparable to the drugs market. According to Europol, in 2015 migrant smuggling in the EU produced profits equal to an estimated €4.7 to 5.7 billion euros[356]. The structure of the OCGs dealing with migrant smuggling does not present just one fixed model, rather it shows different configurations – the hierarchical, loose networks, individual and mixed types[357] – all characterised by high level of organisation and coordination. Among the migrant smuggling routes towards Europe, the most relevant are: the Central Mediterranean route, from North Africa to Italy; the Eastern Mediterranean route, from Turkey to Greece; the Western Mediterranean route, from Morocco to Spain. Other trajectories exploited are represented by the Black Sea route, from Turkey to Romania and Bulgaria, the Western Balkans route towards Central Europe and the 6.000 km of European Union's eastern border.

Moreover, an illicit market linked with migrant smuggling is represented by the trafficking in human beings (THB), which is expected to increase in the next years, thus being a priority on the European security agenda, particularly since 2016, when it was found to support terrorist activities. Considering the different forms of THB in the EU, sexual exploitation is the most common covering over half of the cases registered in 2016 (65%), whose main nationalities were Slovenian, Hungarian, Estonian, Croatian and Danish; while labour

[353] Savona Ernesto U. and Riccardi Michele (eds.), *From illegal markets to legitimate business: the portfolio of organised crime in Europe*, (Trento: Transcrime – Università degli studi di Trento, 2015).
[354] United Nations, International Narcotics Control Board, "Chapter III: Analysis of the World Situation" in *Report 2017*, January 2018. Available at: https://www.incb.org/documents/Publications/AnnualReports/AR2017/Annual_Report/E_2017_AR_ebook.pdf.
[355] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *European Drug Report 2018: Trends and Developments*, June 2018. Available at: http://www.emcdda.europa.eu/publications/edr/trends-developments/2018.
[356] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017.
[357] UNODC, *Global Study on Smuggling of Migrants 2018*, June 2018. Available at: https://www.unodc.org/documents/data-and-analysis/glosom/GLOSOM_2018_web_small.pdf.

exploitation accounted for around one quarter (22%) and the victims were mainly Maltese, Portuguese, Czech, Belgian and British nationals[358].

Another security priority within the European agenda is also constituted by the illicit trafficking of firearms, that is particularly threatening due to the fact that they are durable and may circulate for decades and be sold repeatedly. Illicit firearms trafficking generates from diversion from the licit market, whose regulation is those fundamental to counter the problem. According to the data provided by the FIRE project, the seizures of illicit firearms in the EU, between 2010 and 2015, accounted for a total of 19.246 firearms, mainly pistols (34%) and rifles (27%)[359], thus having a considerable impact on the European security. Moreover, the main destination countries are France, Germany, Greece, Ireland, Italy, the Netherlands, Spain and the United Kingdom, where a particular attention should be placed by law enforcement authorities to counter the problem; while, the main origin countries are the Balkans and countries belonging to the post-Soviet space. A new trend that has been observed and worth mentioning is also the exploitation of the Internet as a facilitator for illicit firearms trafficking, through the purchase of firearms on darknet marketplaces (e.g. Armory, Euroguns, Middle Heart, Nucleus).

Another significant threat on the European security is that one of cyber-dependent crimes. The OCGs active in those crimes and operating in the EU are mostly involved in the following activities: Crime-as-a-Service (Caas), development of malware and cryptoware, network attacks; identity theft and fraud schemes[360]. Several OCGs are also involved in property crime, where an increase targeting of low-level commercial premises has been registered, due to the lower security measures at disposal, as well as a growing use of the illicit online marketplaces to sell stolen goods and the use of the Internet as a facilitator for the commitment of crimes, through the monitoring and analysis of the targets by means of social media platforms. A considerable size of the market is also represented by the online trade of cultural goods, that accounts annually for a total value ranging from €64 to 318 billion euros[361]. Moreover, according to the European Union Intellectual Property Office (EUIPO) a further increase has also been registered in intellectual property crime, through trade in counterfeited and pirated goods, which accounts for a total of €121 billion euros in the EU during 2018[362]. In this case as well, a recent trend observed relates to the use of small parcels and of illicit online marketplaces.

---

[358]European Commission, *EU Data collection on trafficking in human beings in the EU*, Brussels, 2018. Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181204_data-collection-study.pdf.

[359] Savona Ernesto U. and Mancuso Marina (Eds.). 2017. *Fighting lllicit Firearms Trafficking Routes and Actors at European Level. Final Report of Project FIRE*, (Milano: Transcrime – Università Cattolica del Sacro Cuore, 2017). Available at: www.fireproject.eu.

[360] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, 2018. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

[361] European Commission – Directorate-General for Education, Youth, Sport and Culture, *Illicit trade in cultural goods in Europe. Characteristics, criminal justice responses and an analysis of the applicability of technologies in the combat against the trade*, (Luxembourg: Publications Office of the European Union, 2019). Available at: https://publications.europa.eu/en/publication-detail/-/publication/d79a105a-a6aa-11e9-9d01-01aa75ed71a1.

[362] EUIPO-EUROPOL, *Intellectual Property Crime Threat Assessment 2019*, 2019. Available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/2019_IP_Crime_Threat_Assessment_Report.pdf.

Furthermore, another sector where OCGs in the EU are investing is represented by environmental crime, particularly in the illegal trafficking of waste and endangered species, thus damaging the environment as well as the legitimate economy, causing losses of income to legal businesses and loss of tax revenues.

II. In the second part of the thesis the case of the Russian Organisation ("*Rossijskaja Organizacija*") have been analysed in detail, in order to highlight the challenge placed by the infiltration of organised crime in the European legitimate economy. Taking into consideration the contemporary *Rossijskaja Organizacija*, a fundamental dimension that needs to be discussed is related to its historical and cultural background. For this reason, an historical *excursus* is provided in chapter two, since the origin of the contemporary *Rossijskaja Organizacija* traces back to the tradition of the *vory v zakone* ('thieves-in-law'), which emerged during the Soviet times from the development of a criminal subculture that was already present during the Tsarist years. The analysis of the historical origins is relevant for a number of factors, among which the capacity of the *Rossijskaja Organizacija* to adapt itself to the changing conditions of the society as well as for the persistence of old traditions such as the use of a common fund ('*obščak*') – to which all the members of the criminal community had to pay a contribution, that is still one of the characteristics of Russian organised criminal networks – and to highlight the relevance of the prison system, where the *vory v zakone* originated, that is still nowadays a preferential site for recruitment of new members and for the forging of alliances. In this context, another aspect has been investigated in the present research, that one of the language. As observed by Whilelm von Humboldt, a language is the phenomenal manifestation of the spirit of the people[363], therefore, according to the Prussian scholar, to understand a nation it is fundamental to know the language, since it represents the way a people perceive the reality and elaborate about themselves and the others. This interpretation can be applied to specific social groups as well and, in this thesis, it has been applied to the Russian criminal language, the so-called *ofenskij jazyk* or *fenja*, whose origin traces back to the Middle Ages and that, even if radically transformed throughout the centuries, is still spoken within the Russian criminal community and it is still perceived to be a threat, as demonstrated by a law emanated in the Russian Federation in 2013 prohibiting the use of *fenja* in prisons[364]. Therefore, paying attention to the *fenja* language and to the criminal jargon in general means to acquire a deeper and more comprehensive knowledge of the Russian criminal phenomenon. *Fenja* has been defined a *tajnyj jazyk* or *potajnoj jazyk* ('secret language'), since its main functions are secrecy and the unintelligibility for those outside the criminal underworld. There is a whole vocabulary in *fenja* used to indicate law enforcement authorities, such as the words: *musor* ('garbage') from the Hebrew mùser, 'guide'; *ment*, from the Hungarian name for the jacket of the Austro-Hungarian army's uniform (*mente* in Hungarian and *mentik* in Russian), a term employed in the Gulags to indicate the jailor[365]. There is also a set of words to

[363]Von Humboldt Wilhelm, "Latium und Hellas oder Betrachtungen über das classische Alterthum", in *Ausgewählte Schriften* (Berlin: Zenodot Verlagsgesellschaft mbH, 2014).
[364] Gazeta.ru, *Minjust zapretil arestantam materit'cja i «botat' po fene»*, 14th Janyary, 2016. Available at: https://www.gazeta.ru/social/news/2016/01/14/n_8117915.shtml.
[365] Gračev M. A., Mokienko V. M., *Russkij žargon. Istoriko-ètimologičeskij slovar'*, (Moskva: Ast-press, 2009).

denominate the criminal, such as *žul'ban* (compound of the two Russian words: *žul'*, from the Moscow dialect, with the meaning of 'thief, fraudster' and *ban,* 'mob, gang') or *Jurik* (from the verb of the criminal jargon *iurit'* which means in English 'rush around') and a specific vocabulary for the different criminal roles, such as the words *kryša* ('the protector') to indicate criminals which exercised control over given commercial activities, *blatnoj* to indicate someone who has close contacts with a superior or *šestërka*, a low-level criminal[366]. Moreover, an interesting aspect, is the use of the criminal jargon in relation to the drug market, since the *Rossijskaja Organizacija* is particular active in that domain and where, for each product is present a set of names in the criminal jargon, such as *Griša* or *tëmnyj* ('dark') to indicate heroin, *Nikolaj Nikolaevič* or *sneg* ('snow') for cocaine, *Fedja* (Russian diminutive of the male personal noun *Fëdor*) or *skorost'* ('speed') for amphetamines[367], just to mention a few of them.

Furthermore, the cultural analysis is also extended to another distinct feature of the *Rossijskaja Organizacija*, namely the symbology of the criminal tattoos, which characterised Russian criminals in the origin and that are relevant to understand the Russian criminal subculture, whose traits are still partially preserved in the contemporary outlook of the *Rossijskaja Organizacija*. The Russian tradition of criminal tattoos traces back to Tsarist times, where it was frequent to mark physically the criminals, a tradition that was maintained also in the hard-labour camps, where it was common to apply tattoos like '*vor'* ('thief') to convicts and where, in particular during the Stalinist period (1924-1953), the tattoos became a manifestation of the unwritten law of the Soviet prison system. One of the main functions of Russian criminal tattoos was to distinguish the different ranks among the criminals, for instance, a two eight-pointed stars on the chest or on the shoulders meant that the wearer was a high-level criminal. Moreover, there are specific tattoos indicating criminal offenses committed by the wearer, whose meanings changed through the years, for example, the spiders were originally used to underline the commitment of an individual to the criminal life, while nowadays they symbolise involvement into the drug business. Therefore, having a knowledge about the meaning of these marks, allows us to capture details that otherwise would not have been noticed and that are useful to reconstruct the general picture and to understand and counter the threat represented by the *Rossijskaja Organizacija* in Europe.

III. In chapter three the infiltration of the *Rossijskaja Organizacija* in Europe has been considered. As stated by Ulrich Beck, we are living in a "new modernity", where the most characterising aspect of the society is the perception of the risk and its management[368]. With the collapse of the Soviet Union in 1991 the perception of an uncontrollable risk and the feeling of insecurity permeated the European continent, which was overwhelmed by movements of people coming from the Eastern side of Europe. It was exactly in that period that the emergence of the *Rossijskaja Organizacija* was registered in Europe, that was considered as the legacy of the

[366] Ibidem.
[367] Corbelli Michela, *Traducibilità del gergo criminale russo nelle intercettazioni telefoniche in Italia*, (Milano: Fondazione Milano, 2013).
[368] Beck Ulrich, *Risk Society. Towards a New Modernity*, (London: Sage, 1992).

"evil empire", characterised by all those features typical of the Soviet Union, namely the strive for power, expansionism, brutality, lack of scruples and technological expertise.

In the present research the terminology of *Rossijskaja Organizacija* has been proposed, despite the presence of other definitions in the literature, since it is believed to be more accurate. In fact, the first term of the syntagma ('*Rossijskaja'*), refers to something belonging to the Russian culture, without being ethnically Russian and thus encompassing the intrinsic multi-ethnicity of the phenomenon in analysis; while, the second term ('*Organizacija'*) is considered more accurate than other definitions proposed in the literature such as "groups" or "mafia", the first being to generic and the second inaccurate, due to the fact that according to this thesis the *Rossijskaja Organizacija* cannot be associated with mafia-like structures. The *Rossijskaja Organizacija* lacks the high degree of centralisation and the tight hierarchical structure typical of conventional mafia networks, rather it presents a fluid nature[369]. Moreover, the role played by ethnicity and familial ties in mafia structures is not substantial in shaping the Russian criminal networks, where the main drivers for the building of a network is represented by the shared interest in criminal activities and the mutual benefits thereof, while family and ethnicity are just secondary issues. The emergence of the *Rossijskaja Organizacija* in Russia was the result of the imperfect transition from a state-run to a market economy in the aftermath of the fall of the Soviet Union. The main beneficiaries of the transition were a class of enterprise managers, composed by former criminals and known as the "oligarchs", which were able to take advantage of the controversial privatisations under the presidency of El'cin (1991-1999), which controlled the Russian economy through the establishment of corruption networks and criminal activities, specifically in the financial and banking domains. A turning point was represented by the rise to the power of Vladimir Putin, since the 2000s, with the introduction of the so-called *vertikalnaja sistema* ('vertical system'), a process of partial nationalisation of the main industrial sectors (e.g. energy) of strategic relevance for the Russian Federation. In this context, the Russian criminal-business class was compelled to agree on a new type of relation with the State, based on the redistribution of the political and economic power[370] and the subordination of the oligarchs to the State. Moreover, this had consequences on the European security as well, in fact, due to the tight grip exercised by the Kremlin over the national businesses, a considerable amount of capital was moved abroad, specifically in Europe, where Russian capitals of unknown or unclear origin were injected in the banking and financial systems, thus placing a serious challenge to the European legitimate economy. Moreover, the threat of the *Rossijskaja Organizacija* in Europe is further exacerbated by the presence of a strong relation established with the Russian state apparatus, called in the present thesis the "criminal-governmental nexus". According to this assumption, the *Rossijskaja Organizacija* is a tool at disposal of Moscow to pursue its geopolitical agenda and destabilise Europe in the context of the long-lasting confrontation between the European and Eurasian sides of the continent. Considering the characteristics of the *Rossijskaja Organizacija*, a first aspect that should be

[369] Finckenauer James O., Voronin Yuri A., *The Threat of Russian Organized Crime*, Issues in International Crime, NCJ 187085, June 2001.

[370] Karpanos Ilona, *The Political Economy of Organised Crime in Russia: The State, Market and Criminality in The Ussr and Post-Soviet Russi*a, (London: Department of International Politics, 2017).

mentioned is that it does not present a homogenous character, nor within the Russian Federation, neither in Europe. As analysed by Kegö and Moclean[371], there are different configurations, which can be ascribed to the following main models: hierarchical structure, loose affiliations, semi-autonomous and independent gangs, individual criminals. A classification is provided by Galeotti[372], according to ethnicity, in two main categories: the Slavic groups, whose major representatives are the *Solncevskaja Bratva* based in Moscow, the *Tambovskaja Bratva* based in St. Petersburg and the *Uralmaš gruppirovka* of Ekaterinburg; the Caucasus groups, which are composed by loose networks of Georgian and Chechen origins.

Moreover, taking into account the infiltration of the phenomenon in Europe, what emerges is that the *Rossijskaja Organizacija* is mainly involved in high-level crimes, specifically in the financial and banking systems, the luxury market, import-export businesses, real estate, transportation, hotels and restaurants, casinos and night clubs[373]. The main reason why the *Rossijskaja Organizacija* is deeply involved in the legitimate economy relies on the possibility offered to move freely "black money" from Europe to other countries of activity outside the European borders, among which Russia, and to launder the illicit proceeds of criminal operations. Considering the involvement in the illegitimate economy, the *Rossijskaja Organizacija* specialised in the illicit drugs trafficking, where it holds a dominant position in the European heroin market, the illicit firearms trafficking and the human trafficking. However, the main threat placed by the phenomenon to the European security architecture is that one related to the legitimate economy. Money laundering is one of the main activities in which the *Rossijskaja Organizacija* is involved in Europe and two main *modus operandi* are applied: the first one consists in the purchase of property (e.g. real estate) to launder money, while the second method implies the transfer of money abroad in non-EU countries, where there are weaker judiciary and banking systems, which are exploited as preferential channels to launder the money deriving from illicit activities, which are then moved to EU countries and accepted by Western banks. Evidences of the money laundering activities carried out by the *Rossijskaja Organizacija* in Europe are particularly evident in three cases taken into consideration in this thesis: the "Russian Laundromat", the "Magnitskij affair" and the "Nord Stream Case".

The first case, the "Russian Laundromat", is a sophisticated money laundering case of transnational nature, perpetrated through Moldincobank in Moldova, which allowed criminals, corrupted politicians and public officers to move, in the time span ranging from 2010 to 2014, US$ 20 billion from Russian banks to Moldincobank, where the money were first "washed" through the corrupted judicial system in Moldova and then sent to Latvia and other EU countries. Moreover, this case shows another relevant aspect, namely the connivance between the *Rossijskaja Organizacija* and the Russian state, the so-called "criminal-governmental

[371] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 22-28.
[372] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Heaven and London: Yale University Press, 2018).
[373] Shelley Louise, "Contemporary Russian Organised Crime: Embedded in Russian Society", in Fijinaut and Paoli (eds.), *Organised Crime in Europe. Concepts, Patterns and Control Policies in the European Union and Beyond*, (Dodrecht, The Netherlands: Springer, 2004). pp. 563-584.

nexus". In fact, according to the investigation conducted by the Organised Crime and Corruption Reporting Project (OCCRP) in 2014, among the perpetrators of the "Russian Laundromat", there were businessmen with strong and even parental ties with the president Putin and the state security apparatus[374]. Another money laundering case, which evidences even more the "criminal-governmental nexus" is then represented by the "Magnitskij affair", that takes its name from the main victim of the crime, Sergej Magnitskij, deceased in 2009 after being arrested in 2008 and accused of collusion with the Hermitage Capital Management (HCM) fund and its owner Bill Browder, a British businessman. As reported by Galeotti[375], The HCM was a successful foreign fund operating in the investment sector in Russia, with hundreds of millions of dollars as revenues. As a consequence, Bill Browder and the business model of the HCM began to be perceived as a threat by the Russian establishment and competitors, thus the Russian Federation banned Browder to enter the country in 2006. The following year, a raid was organised by the police in the offices of the HCM, in which computers and relevant documents were seized and subsequently exploited to produce false evidences of fraud perpetrated by the HCM, that was requested to pay a tax refund of ₽5.4 billion roubles (US$ 230 millions). The refund was than diverted and allocated to three shell companies from which the money was transferred to the beneficiaries of the criminal operation, among which tax officers, politicians and trustees of Vladimir Putin.

Then, a third money laundering case which highlights the seriousness of the threat placed by the infiltration of the *Rossijskaja Organizacija* in the European legitimate economy is represented by the "Nord Stream case". It involves the flows of Russian money injected in the EU and the corruption networks established during the construction of the Nord Stream pipeline in the Baltic Sea, inaugurated in 2011 and transporting gas from the Russian city of Vyborg to the German city of Greifswald. The project was implemented by a joint Russian-German venture called Nord Stream AG, whose main shareholder is Gazprom[376]. There are a number of aspects that have raised doubts about the management of the project, among which the fact that the Russian parties were not transparent about the estimated cost and in relation to the managers and board members involved in the project in the Western side, which included close friends of Vladimir Putin and former officers of the state security service of the German Democratic Republic.

Furthermore, to evaluate the impact of the infiltration of the *Rossijskaja Organizacija* in Europe, the presence of the phenomenon in Germany, Italy and the Baltic countries has been taken into consideration.

One of the main characteristics of the *Rossijskaja Organizacija* in Germany is the transnational character and the multi-ethnic composition of the criminal networks. According to the analyses of the Bundeskriminalamt

[374] Organised Crime and Corruption Reporting Project (OCCRP), *The Russian Laundromat*, 22nd August 2014. Available at: https://www.reportingproject.net/therussianlaundromat/russian-laundromat.php.
[375] Galeotti Mark, *The Vory. Russia's Super Mafia*, (New Heaven and London: Yale University Press, 2018). pp. 215-217.
[376] Gazprom, *Gas Pipeline: Nord Stream. The gas pipeline directly connecting Russia and Europe*, 2012. Available at: https://www.gazprom.com/projects/nord-stream/.

(BKA)[377] 73.7% of the activities of the *Rossijskaja Organizacija* based in Germany were conducted internationally. Moreover, the phenomenon presents a strong connection with the autochthone criminal underworld and the different ethnicities involved in organised crime, among which most notably the Lithuanians. Another feature that has been detected is the high involvement of the *Rossijskaja Organizacija* in cybercrime activities, where it holds the largest share of crimes committed over the whole figure for 2017 (52.9%)[378]. The main activities carried out in the cyber domain are represented by digital blackmail (29.4%) and attacks on online banking systems (23.5%)[379]. Moreover, it presents a high level of specialisation in the use of cryptocurrencies (e.g. Bitcoin) and the exploitation of Internet illicit marketplaces (e.g. Darknet) for the trafficking of illicit goods. The main branches of the *Rossijskaja Organizacija* in Germany are: the *Tambovskaja Bratva*, present in Düsseldorf and active in money laundering and extortion activities as well as exerting control over the night club and prostitution markets; the *Kiolnskaja Bratva* based in Cologne and involved mainly in the illegal trafficking of drugs and weapons[380]; the *Dolgoprudenskaja* gang, specialised in extortion crimes[381] and a number of independent criminal clusters operating mainly in the cities of Hamburg and Frankfurt am Main.

The second case study for the analysis of the infiltration of the *Rossijskaja Organizacija* in Europe is represented by Italy, where it is mainly active in the legitimate economy. Moreover, a divide is present in term of ethnicity, with the Slavic groups operating in the North-eastern regions of the country (Emilia-Romagna, Marche, Tuscany and Veneto), involved in money laundering and investments activities mainly in the real estate sector; while the Caucasus groups are active in the Southern regions, where they are involved in property crime and extortion. As far as their *modus operandi* is concerned, it is worth mentioning that particularly in Italy, where strong organised crime groups and mafia networks are well rooted in the territory, the *Rossijskaja Organizacija* it is not interested in establishing an hegemonic control over the territory, rather the main aim is to build close relationships with the political and bureaucratic spheres, in order to gain protection for the activities deployed. According to the investigations conducted by the *Direzione Investigativa Antimafia (DIA)*[382] – the Italian anti-Mafia investigation body – the main threatening branches of the *Rossijskaja Organizacija* operating in Italy belong to Georgian nationality, which are extensively present in the Southern region of Apulia, in the city of Bari, where the *Kutaisi* and *Rustavi* clans are involved in property crime,

[377] Bundeskriminalamt (BKA), *Organisierte Kriminalität, Bundeslagebild 2017*, 1st August 2018. Available in German at: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html.
[378] Ibidem.
[379] Ibidem.
[380] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 29-31.
[381] Telegraf.rs, *Ruska mafija važi za najopasniju na svetu: Vlada surovim metodama, ima 300.000 članova, a njihove veze sa državom su veoma moćne*, 9th October 2017. Available in Serbian at: https://www.telegraf.rs/zanimljivosti/svastara/2902316-ruska-mafija-vazi-za-najopasniju-na-svetu-vlada-surovim-metodama-ima-300000-clanova-a-njihove-veze-sa-drzavom-su-veoma-mocne.
[382] Direzione Investigativa Antimafia (DIA*), Relazione del Ministro dell'Interno al Parlamento sull'attività svolta e sui risultati conseguiti dalla Direzione Investigativa Antimafia*, Luglio – Dicembre 2018. Available at: http://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html.

extortion, drug trafficking and exploitation of the prostitution. It is also interesting to notice that the Georgian groups differentiate themselves from the Slavic groups in terms of organisational structure, which results to be based on a tight hierarchy and paramilitary methods. Another minor group active in Italy is also represented by criminals of Ukrainian nationality, mainly active in the South of the country and involved in migrant smuggling and sexual and labour exploitation[383].

The last case study considered is that one of the Baltic countries, namely Estonia, Latvia and Lithuania. These countries represent a specific case, due to the fact that in their territory the *Rossijskaja Organizacija* should be considered an indigenous problem, rather than an exogenous one. In fact, a large historical community of ethnic Russians is registered in all the Baltic countries and especially in Latvia, that act as a facilitator for the penetration of the *Rossijskaja Organizacija* in the territory[384], whose main activities in the Baltic area are represented by money laundering activities, investments in the real estate sector, cybercrimes as well as illicit drug trafficking and smuggling of stolen goods, particularly through the Riga port and the Lithuanian border with the Russian exclave of Kaliningrad.

IV. In chapter four the threat placed by the activities deployed in the cyber domain by the *Rossijskaja Organizacija* has been addressed in depth. There is never enough security that can be provided to a system, a company or a country, security needs to keep pace with the global changes and, particularly, with the rising of new technologies, which expose us to new and unknown vulnerabilities. The cyber domain is a preferential site for the implementation of the technological progress and it is considered a priority in the security agenda. According to a research conducted by CLUSIT in 2018 an increase of +77.8% of cyber-attacks has been recorded, if compared to 2014 and +37.7% if compared with 2017[385]. The main categories of cyber-attacks are the following: cybercrime, cyberespionage, cyberwarfare and hacktivism. Taking into consideration the case of the cyber threat placed by the *Rossijskaja Organizacija* to the European security it is worth mentioning that, according to the Russian military doctrine[386], cyberwarfare is officially included in the *Informacionnaja Vojna* ('Information Warfare') conducted by the Russian Federation to defend its national interests and pursue its goals. In the Russian exegesis Information Warfare is a much broader concept than cyberwarfare, including not only electronic warfare and computer network operations but also psychological, information and disinformation operations. Thus, cyberwarfare in Russia is considered as part of a wider strategy developed during the Soviet times which changed only in the means employed, however the reasons, tactics and the targets have remained the same. Moreover, in the Russian context, from all the three main interpretations of

[383] Ibidem.
[384] Kegö Walter, Moclean Alexandru, *Russian Speaking Organized Crime in the EU*, (Stockholm: Institute for Security and Development Policy, 2011). pp. 47-50.
[385] Clusit, *Rapporto 2019 sulla Sicurezza ICT in Italia*, 2019. Available in Italian at: https://clusit.it/rapporto-clusit/.
[386] Presidential Decree No.2976, *The Military Doctrine of the Russian Federation*, 25th December 2014. Available in Russian at https://rg.ru/2014/12/30/doktrina-dok.html and available in English at https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf.

the Information Warfare discussed in the research (the "subversion-war" developed by Messner, the "net-centric war" of Dugin and the "information warfare" elaborated by Panarin), what emerges is the perception among the Russians of an on-going confrontation with the West, whose main aim is the manipulation of the informational dimension. Therefore, the cyber domain is considered of the utmost importance both as a defensive and offensive system at disposal to the Russian Federation to defend itself. The ideological framework is fundamental to understand the characteristics of the *Rossijskaja Organizacija*, most notably the degree of connivance with the State, with whom a relation of mutual benefits has been established, based on profits for organised crime in exchange of engagement in activities which have a benefit for the State, such as cyber-attacks directed towards public and private targets belonging to the West. The "criminal-governmental nexus" is clearly visible in three episodes in particular where Russia was involved, namely the diplomatic clash with Estonia (2007), the military conflict in Georgia (2008) and Ukraine (2013-present), which have served as grounds to test Russian cyber capabilities and tactics. In the case of Estonia, DDoS (Distributed Denial-of-Service) attacks were launched against Estonia's internet websites, making the country unable to communicate with the outside. The reason behind this attack was a form of retaliation of Russia against the decision to move the statue of a Soviet soldier from its original position in Tallinn, a measure that was highly criticised by Russia and the ethnic Russian community living in Estonia, considering it an outrage to the sacrifice of Soviet soldiers for the liberation of Estonia from Nazism. Then, the second case involves DDoS attacks against Georgia's governmental, economic and communication networks as well as telecommunication providers, in the context of the Russian military intervention in South Ossetia and Abchazia. A further example showing Russia's cooperation with hacking groups is represented by the on-going conflict in Ukraine, started in 2013, where an extensive and coordinated cyber strategy has been applied by Russia, with the aim of destabilising and disorienting the country, compromising the legitimacy of the Ukrainian political and military institutions as well as their capacity to operate and communicate through the deployment of cyber-attacks able to open backdoors in the Ukrainian governmental systems (e.g. advanced malware "Ouroboros") and even infiltrate the power centre networks (e.g. cybersurveillance tool "BlackEnergy"). Further evidences of the "criminal-governmental nexus" are also provided by the analysis of the Advance Persistent Threat (APT) groups, particularly of APT28 and APT29. APT attacks are characterised by specific targets (mainly civilian targets in the last years), a high level of organisation, adaptation to the defenders' countermeasures and long-term campaign of attacks[387]. Two APT groups are allegedly associated with the Russian Federation, namely: APT 28, that is believed to be linked with Unit 26165 and Unit 74455 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Russia's military intelligence; APT 29, supposedly associated with the Russian Federal Security Services (FSB) and the Foreign Intelligence Service (SVR). The evidences which support the thesis of the link between APT28 and APT29 with the Russian state

[387] Chen Peng, Desmet Lieven, Huygens Christophe, "A Study on Advanced Persistent Threats" in De Decker B., Zúquete A. (eds*) Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science*, vol 8735. (Berlin, Heidelberg: Springer, 2014), 63-72. Available at: https://link.springer.com/chapter/10.1007/978-3-662-44885-4_5#citeas.

are based on a number of indicators, among which: the analysis of the targets, which are of interest for the Russian Federation; the fact that significant components of both APT28 and APT29 were compiled in Russian language; moreover, most of the malware samples attributed to APT28 and APT29 were compiled during working days between 8AM and 6PM in the UTC+3 time zone, corresponding to the working hours in Moscow and St. Petersburg[388]. Furthermore, a fundamental aspect worth mentioning is the merger between old Soviet tactics and new technologies in the Russian cyber strategy. This element is clearly visible in the fact that attacks are not intended to destroy a target, rather to undermine the adversary's strategy, create confusion, destabilise and compel the target to focus on a specific damage caused, that turns to be not the primary Russians' aim, rather the secondary one, allowing them to attack their original primary target, while the adversary is distracted and fully engaged in defending the secondary objective. This is a pattern already present in the past with the old Soviet military principle called *maskirovka*, also known as Russian military deception, which is now applied to the cyber domain and employed predominantly to achieve political and geographical gains without engaging in an open military confrontation with the enemy, as a form of maskirovka 2.0[389].

V. As observed by the Serious and Organised Crime Threat Assessment (SOCTA) report[390], organised crime is a key threat to the European security architecture, generating each year billions of euros in profits through the activities carried out in the European Union. Moreover, it has become more sophisticated in the methods employed, most notably in the financial and banking sectors. Based on the analysis conducted by Europol, five key priority threats to tackle organised crime have been listed, namely: cybercrime, drug trafficking, organised property crime, migrant smuggling and trafficking in human beings. At the EU level the strategic framework for the implementation of the security measures is represented by the European Agenda on Security 2015-2020, adopted by the European Commission in 2015, that sets out the three main pillars for action in the security field where the EU can bring an added-value: information sharing between national law enforcement authorities and the EU agencies, cooperation at the operational level, supporting action. Furthermore, the commitment of the European Union in the fight against organised crime is shown by the EU Policy Cycle, a four-years policy initiative launched for the first time in 2010 to provide a coordinate and more effective response. In 2017 the Council of the European Union has adopted the EU Policy Cycle 2018-2021, where are listed the ten key priority areas to tackle organised crime as follows: cybercrime, drug trafficking, facilitation of illegal immigration, organised property crime, trafficking in human beings, excise and fraud, illicit firearm trafficking, environmental crime, criminal finances and money laundering, document fraud. Moreover, further

[388] FireEye Threat Intelligence, *APT28: A Window into Russia's Cyber Espionage Operations?*, 2014. Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.
FireEye Threat Intelligence, *HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group*, 2015. Available at: https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html.
[389] Roberts James Q., *Maskirovka 2.0: Hybrid Threat, Hybrid Response*, (Florida: Joint Special Operations University Center for Special Operations Studies and Research, December 2015). Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1007494.pdf.
[390] Europol, *European Union Serious and Organised Crime Threat Assessment (SOCTA*), 2017. Available at: https://www.europol.europa.eu/socta/2017/.

initiatives have been taken by Europol with the Strategy 2020, where it is laid down its commitment to become the EU criminal information hub, deliver operational support, be a platform for European policing solutions, be at the forefront of law enforcement innovation and research and be the model EU law enforcement organisation[391]. The main operations of Europol to counter the threat of organised crime are deployed through the European Serious and Organised Crime Centre (ESOCC), which provided over 3.445 intelligence analysis and supported 612 operations in 2018[392].

Furthermore, a particular attention has been devoted to the needed measures to counter the problem represented by money laundering activities and cybercrime. As far as the first element is considered, in 2018 the European Union adopted the 5th EU Anti-Money Laundering Directive (AMLD), which introduced substantial amendments to the European Union Anti-Money Laundering System, such as the setup of central bank account registers in all Member States and publicly available registers for companies, the improvement of the EU Financial Intelligence Units (FIUs), the increased cooperation between anti-money laundering supervisors and the European Central Bank (ECB) and the limitation of anonymity guaranteed by virtual currencies,

Considering the measures to tackle cybercrime, the main priorities set by the EU Cybersecurity strategy, launched in 2013, have underlined the need to improve cyber resilience and elaborate an EU cyber defence policy. Moreover, at the legislative level, the cornerstone of the EU legislation on cybersecurity is represented by the Directive on Network and Information Security, also known as NIS directive (EU Directive 2016/1148), adopted in 2016, which provided the establishment of a Computer Security Incident Response Teams (CSIRT) and a national NIS Authority for each Member State as well as the requirement to set coordinated action plans for strategic economic sectors such as banking, digital infrastructures, energy, financial market infrastructures, healthcare, transport and water[393].

In conclusion a set of policy recommendations has been proposed in the thesis to counter the impact of the phenomenon analysed. Taking in consideration organised criminal groups in Europe the most relevant policy recommendations are:

- the elaboration of common regulations over online platforms and applications, which are employed as facilitators for the activities of organised criminal groups;

[391] Europol, *Europol Strategy 2020*, Vienna, 13th December 2018. Available at: https://www.europol.europa.eu/publications-documents/europol-strategy-2020.
[392] Europol, *Europol Programming Document 2019-2021*, adopted by Europol Management Board on 30th November 2018, The Hague, 29th January 2019. Available at: https://www.europol.europa.eu/publications-documents/europol-programming-document.
[393] European Commission, *EU cybersecurity initiatives. Working towards a more secure online environment*, Brussels, 2017. Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.

- increased control should be applied to Belgium, Spain and the Netherlands, main entry points in Europe for cocaine trafficking and enhanced supervision is needed in the European terminal points of the heroin-routes, such as: Bulgaria and Croatia for the "Classic Route"; Romania, Hungary, Austria and Slovakia for the "Northern Route"; Greece and Italy for the "Southern Route";
- enhanced control over the European Union's Eastern border (including Norway, Finland, Estonia, Latvia, Lithuania, Poland, Slovakia, Hungary, Bulgaria and Romania) to counter migrant smuggling;
- higher control and regulation over the most targeted economic sectors employed by organised crime groups to deploy human trafficking activities (e.g. agriculture, cleaning services, construction, transportation) and specific attention should be placed on Slovenia, Hungary, Estonia, Croatia and Denmark for sexual exploitation, while on Malta, Portugal, Czech Republic and Belgium for labour exploitation;
- the elaboration of common standards for the reactivation of deactivated firearms and monitoring over illicit online market platforms (e.g. Dark web), where firearms are purchased.

Then, considering the threat placed by the *Rossijskaja Organizacija* to the European security, the main policy recommendations proposed are the following:

- a focus on the financial and banking systems, in which the continuous evolution of the technological tools at disposal in the cyber domain has been exploited to deliver new and ever-changing patterns of attack;
- a specific attention on money laundering activities in the EU, particularly in the Nordic and Baltic countries, preferential sites for the operations deployed, with the establishment of an effective mechanism to demonstrate the owners of specific structures and capital invested in the EU as well as the clear origin of the money flows and the imposition of fines to pressure and incentivise continual surveillance by the banks themselves;
- heightened attention should be placed on the Russian expatriate communities in the EU, which must be considered a priority area for security as well as assiduous monitoring of the European prisons system should be implemented, since it is exactly during the conviction period that new members are recruited by Russian organised criminal networks;
- the establishment of dedicated units within the police agencies in the EU countries most affected by activities carried out by Russian criminals and the creation in the EU of a cross-departmental body focused on Russian organised crime within Europol.

From the analysis conducted in this thesis results that the threat placed the *Rossijskaja Organizacija* should be placed on the priority agenda of the European Union, due to the increasingly evolving nature of the

phenomenon and the high degree of adaptability to the different contexts demonstrated in the case studies analysed. Moreover, as a result of the research conducted, the following conclusions have been elaborated:

- the phenomenon cannot be completely associated with mafia-like structures; thus, the countermeasures should be developed according to this assumption;
- the presence of a "criminal-governmental nexus" in the Russian Federation between the *Rossijskaja Organizacija* and the state apparatus, with consequences on the effects of the phenomenon in Europe;
- the most relevant threat posed by the *Rossijskaja Organizacija* in Europe is that one deriving from the activities conducted in the legitimate economy, specifically in the financial and banking systems by means of fraud and money laundering schemes;
- the *Rossijskaja Organizacija* is employed as a tool of the Information Warfare (IW) conducted by the Kremlin to pursue its geopolitical agenda and destabilise Europe in the context of the long-lasting confrontation between the European and Eurasian sides of the continent.

Moreover, due to the specific features of the *Rossijskaja Organizacija* analysed, a fundamental aspect that should not be underestimated in the implementation of an effective approach to counter the threat placed by the phenomenon is constituted by the cultural dimension, involving the knowledge of Russian history, politics and strategic culture, which enable us to be aware of the variables shaping the contemporary outlook of the *Rossijskaja Organizacija* and to provide an interpretation of its distinctive features, tactics and targets. It is only through a deep and complete analysis of the phenomenon, involving the observation of the finest and of apparently not relevant details, that is possible to see the global picture, truly understand the problem and develop the effective measures required to counter it.