This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 700688.

TAKEDOWN

Identify . Prevent . Respond

UNDERSTAND THE DIMENSIONS OF ORGANISED CRIME AND TERRORIST NETWORKS FOR DEVELOPING EFFECTIVE AND EFFICIENT SECURITY SOLUTIONS FOR FIRST-LINE-PRACTITIONERS AND PROFESSIONALS

Deliverable D2.6

European Baseline report on current OC/TN specifics and collection of sources

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 700688.

Project

Acronym: TAKEDOWN

Title: UNDERSTAND THE DIMENSIONS OF ORGANISED CRIME AND TERRORIST NETWORKS FOR DEVELOPING EFFECTIVE AND EFFICIENT SECURITY SOLUTIONS FOR FIRST-LINE-PRACTITIONERS AND PROFESSIONALS

Coordinator: SYNYO GmbH

Reference: 700688

Type: Research and Innovation Action (RIA)

Program: HORIZON 2020

Theme: Investigating the role of social, psychological and economic aspects of the processes that lead to organized crime (including cyber related offenses), and terrorist networks and their impact on social cohesion

Start: 01. September 2016

Duration: 36 months

Website: http://www.takedownproject.eu

Consortium: **SYNYO GmbH (SYNYO)**, Austria
Fundación Euroárabe de Altos Estudios (FUNDEA), Spain
Universitat Autònoma de Barcelona (IDT-UAB), Spain
Middlesex University (MU), United Kingdom
University of Leeds (UNIVLEEDS), United Kingdom
ETH Zurich – Center for Security Studies (CSS), Switzerland
Technion Israel Institute of Technology (TECHNION), Israel
Czech Technical University (CVUT), Czech Republic
Technische Universität Darmstadt (TUDA), Germany
Agenfor Italia (AGENFOR), Italy
Center for the Study of Democracy (CSD), Bulgaria
Peace Action Training and Research Institute of Romania (PATRIR), Romania
University of Security Management in Kosice (VSBM), Slowakia
Leuven Security Excellence Consortium vzw (LSEC), Belgium
Agency for European Integration & Economic Development (AEI), Austria
Valencia City Council - Local Police (PLV), Spain
Police Academy in Szczytno (WSPol), Poland
Cloud security Alliance (CSA), United Kingdom

Deliverable

Number:	**D2.6**
Title:	**European Baseline report on current OC/TN specifics and collection of sources**
Lead beneficiary:	FUNDEA
Work package:	WP2 Analyse: Base Research, Model Comparison, Stakeholder Mapping, and Solution Ecosystem
Dissemination level:	Public (PU)
Nature:	Report (RE)
Due date:	30.6.2017
Submission date:	30.6.2017
Authors:	**Pablo Martín Rodríguez**, FUNDEA
Contributors:	**Lucas J. Ruiz Díaz**, FUNDEA **Javier Ruipérez**, FUNDEA **Inmaculada Yuste**, FUNDEA **Inmaculada Marrero**, FUNDEA **All Partners**
Reviewers:	**Florian Huber,** SYNYO

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 700688.

Table of Content

Executive Summary

TAKEDOWN Project aims to improve the European response to both forms of criminality in terms of designing effective preventative and responsive strategies and public policies, identifying best practices and most efficient tools for preventing and countering them, disseminating this knowledge among the different stakeholders involved and enhancing their cooperation and mutual cross-fertilization, ultimately offering the victims and the European general public means to get aware of these threats and risks as well as the tools and instruments at their disposal to defend themselves therefrom.

This Baseline Report on Organised Crime (OC) and Terrorist Network (TN) specifics presents the results of Task Force 2, whose aim is essentially to set the analytical fundamentals for TAKEDOWN Project. It builds thus on its previous TAKEDOWN Deliverables: (2.1) OC/TN literature review, (2.2) OC/TN model comparison, (2.3) key representative and stakeholder's mapping, (2.4) OC/TN response screening, and (2.5) collection of digital and public service security solutions.

OC/TN have become two matters of great concern for European governments and societies affecting social cohesion at both European Union (EU) and member state (MS) levels and calling for a response as effective as well grounded in European social and political values. This is a key notion because the profound impact of OC and TN needs to be measured not only by the economic and social harm they inflict upon European societies and economies but also by the costs that countering OC/TN has on those very same societies and economies in terms of political legitimacy, social cohesion and public expenditure. The review of strategies, policies, practices and measures put in place for countering OC/TN has shown that full compliance with fundamental rights is critical to assure this legitimacy and consequently guaranteeing ongoing public support.

The landscape of OC and TN within the EU presents a complicated situation that demands decisive public action but also discerning circumspection. Despite the undeniable social unrest that terrorism causes in every society beaten by an attack or the critical challenge that terrorism implies to a democratic political order, European societies are, compared to other parts of the world, relatively safe, as quantitative studies prove beyond doubt. Terrorism within the EU is largely domestic and/or locally based and shows a strong preference for soft targets in line with its unsophisticated modi operandi. This is not to deny its dangerousness, particularly because of its organisation in networked cells loosely connected but to emphasize instead the need to focus on better understanding radicalisation as one of the process that may lead an ordinary citizen to join a terrorist group in Europe or abroad (so called foreign fighters) or turn into a potential lone terrorist actor. On its part, OC is growing increasingly diverse in its methods, structures and impact on society. Criminal markets and services where OC thrives show no downward trend but contrarily a high dynamism in traditional and new ones - drugs, immigrant smuggling, traffic in human beings, financial fraud, counterfeit, environmental crime and others. Internet and new information and communications technologies (ICT) has facilitated the expansion of traditional OC horizon and opened a new highly flexible flat-structured global cybercriminal market.

It is understandable thus that OC/TN have reached an outstanding position in EU and MS political agendas through the consideration that both represent serious threats to European security demanding a common action. Hence, the Renewed EU Internal Security Strategy and the new Global Strategy for the EU's Foreign and Security Policy consider both as major European threats and design

the guidelines for a comprehensive countering response. Those are to be implemented according to the EU legal framework - particularly the Area of freedom, security and justice (AFSJ) - that possesses a high degree of intricacy because of the flexibility and differentiated legal regimes applying to certain MS and the double regulation that still governs EU external action. The institutional security architecture that the EU has progressively established to face these threats shows, on its part, an undesirable complexity liable to hamper the efficacy of the intended response.

Academics and researchers from many different scientific fields have devoted an enormous attention to OC and TN and therefore numerous theoretical models have been suggested. Reviewing scientific literature and screening those models from the point of view of TAKEDOWN project have led to some relevant conclusions that is summarised as follows.

The analysis of the root causes of both phenomena reflects a multi-dimensional factorial portrait that discloses the interaction of those causes along the macro, meso and micro levels enlightening the social construction of both OC/TN with significant consequences as to the pertinence of a systemic approach, the enlargement of preventing measures with an unavoidable multi-agency and multi-stakeholder approach or, epistemologically, the drift from causal to analytical models whose explanatory value lies in a collectively better understanding of these processes even though some models only focus on certain dimensions or interfaces or are built on specific scientific disciplines.

Accordingly, a multi-dimensional understanding of OC/TN is submitted here as the virtuous result of those varied scientific contributions that have revealed key aspects of OC/TN such as the functioning of concrete criminal markets at the international, national or local levels, the existence of a legal-illegal continuum with which OC assures endurance by means of corruption and penetration into the legal economy or the relevance of variables such as trust, violence or gender. Scientific literature has also provided with a variety of theoretical perspectives and models that can explain the extremely diverse structures that OC and TN currently present ranging from highly hierarchical groups to loosely networked cells to even lone actors. Valuable models explaining their functioning and offering useful investigative tools and techniques for law enforcement agencies and authorities accompany those theoretical insights. This is also the case of the intricate process radicalisation that academic literature has dissected so as to understand the different factors and dynamics it involves.

Additional traits of the complexity of current OC/TN is due to the emergence of clear nexus between them that have passed the traditional cross-instrumental rationale - 'methods not motives' - to reach a degree of hybridization in some cases that blurs their once clear-cut difference. Internet and new ICT have profoundly transformed OC/TN supplying new tools and techniques for offline activities, allowing new distributed criminal structures or providing extremely powerful platforms for terror propaganda, training and fundraising. The cyberspace is a new territory where OC/TN develop and thrive, which demands comprehensively rethinking cybersecurity in terms of multi-agency and public-private cooperation, due to its global scale, the emergence of new motivations of atypical criminal offenders or the transformation of criminal and terror structures and methods as well as law enforcement tools and techniques.

All these considerations are pertinent to the main purpose of TAKEDOWN Task Force 2, which is identifying the methodological framework for modelling OC/TN. This framework must meet five different features or methodological modelling directions - namely (a) operational under uncertainty; (b) dynamic-process reflecting; (c) holistic and target-oriented - universally adaptational; (d) open and self-learning; (e) self-reflective - structurally sensitive; and (f) fundamental rights abiding. The

first three are structural requirements of the model, the following two relate to the functioning of the model, while the last one is normative in character. The effects will be a model that expands the stakeholders' horizon to unconventional scenarios in a target-oriented way, avoiding the risks of reification while internalising the different scientific methodological approaches - than are proper to those diverse stakeholders-, allowing for cross-fertilization, ex ante and ex post facto assessment in detecting best practices without endangering social legitimacy.

1. Introduction

Organised crime and terrorist networks (OC/TN) represent first-rank challenges for every society, including current European ones. Both phenomena affect the very core of the social organisation interfering with its public decision-making process and altering the results of its social distributional norms. However the risks and threats to social, political and economic cohesion that OC/TN pose to European societies nowadays have experienced a substantial change due to how those two criminal endeavours have manifested across time and space and how they have adapted to the modification of socio-political and socio-technical conditions prevailing in current European countries.

TAKEDOWN Project aims to improve the European response to both forms of criminality in terms of designing effective preventative and responsive strategies and public policies, identifying best practices and most efficient tools for preventing and countering them, disseminating this knowledge among the different stakeholders involved and enhancing their cooperation and mutual cross-fertilization, ultimately offering the victims and the European general public means to get aware of these threats and risks as well as the tools and instruments at their disposal to defend themselves therefrom.

This objective requires a previous review of the state of the art as to the extensive body of scientific literature that has analysed organised crime and terrorism from many different perspectives and academic disciplines (TAKEDOWN Deliverable 2.1). A preliminary identification of public and private stakeholders involved in this response (Deliverable 2.3) assessing their practices, measures, strategies and policies (Deliverable 2.4) and mapping the digital security solutions and public services available (Deliverable 2.5) has been conducted in order to examine those varied scientific insights and their applicability (Deliverable 2.2), thereby setting the methodological ground for a more thorough empirical research informing the definition of a modelling framework suitable enough to encompass the complexity of both OC/TN and the associated response thereto. This is the chief object and purpose of Task Force 2 of TAKEDOWN to which this Baseline Report is a part.

This European Baseline Report on Organised Crime and Terrorist Network specifics will thus review and present the main results of this Task Force 2. In Section 2 OC/TN will be considered as two major European concerns due to their impact on the social, political and economic cohesion of the European Union (EU) and its member states (MS), their increasingly salient position within the political agenda of the EU that has mirrored the establishing of a prolific institutional framework where remarkable synergies between public and private stakeholders have flourished. In Section 3, the scientific state of the art will be summed up focusing on the different perspectives of analysis and major insights that academic literature has brought to attention and should be taken into account for modelling purposes. This review will allow extracting in Section 4 some relevant conclusions as to the methodological framework where the subsequent development of the model that the TAKEDOWN Project should create and apply.

2. Organised Crime and Terrorist Networks as Major European Concerns

2.1. The Impact on European Societies: Mapping Organised Crime and Terrorist Networks in the European Union

Across successive Eurobarometers on European public opinion, OC/TN remain steadily among EU **citizens' major concerns**. In the last Eurobarometer on European public opinion, terrorism occupies a conspicuous second position and crime gets closer in several MS (EB86, 2016). This opinion does not seem misguided. Although the particular measurement methodology of the impact of OC/TN in the EU might still remain controversial (Levi, 2016) and consequently the concrete figures and amounts that authors, different European research projects and organizations have provided should be taken more as indicators than accurate calculations, there is a widespread agreement on the significant impact of both phenomena on the EU and its MS from many different perspectives.

The **impact of OC on European economies** is patent and ever increasing not only in terms of number and values of confiscated assets but also as to the economic weight of those illegal markets and the profits they yield for those criminal actors (Savona/Riccardi, 2015). In its more recent assessment Europol has risen from 3600 in 2013 to more than 5000 in 2017 the number of internationally active OCG currently under investigation within the EU, although this increase might correlate to refined intelligence within law enforcement authorities (LEAs) and not necessarily to an actual increase of OC activities and/or economic value (Europol, 2017a). Focusing on OC costs, a report conducted for the European Parliament identified minimum total costs of OC activities in the EU to be EUR 126.3 billion with specific calculation for several areas such as homicide, illegal drugs, fraud against the EU, environmental crime and others, showing that reliable data are missing in many instances and that these costs are highly dependent on other public choices such as health policy (e.g. regarding drugs consumption). More importantly it highlights the need to take into account the **costs of responding to OC** and also to keep in mind the inherent limits of this approach in order to assess the social impacts of OC, many of which remain intangible (Levi et al., 2013). The EFFACE EU Project dealing with environmental crime is extraordinarily illustrative of the above-mentioned problems when measuring and quantifying "costs" and "impacts" (Illes et al, 2014). The ability, if not the necessity, of OC to infiltrate into the legal economy and to skew the normal functioning of public institutions through corruption undoubtedly impairs the legitimate distribution of social costs and welfare in EU member states and distorts the social perception of these democratic systems undermining their legitimacy. The extensive public response to this threat in terms of public expenditure, institutional framework or social consequences of countering strategies and police measures is in itself definitive proof of the profound impact that OC has on European societies.

When measuring **terrorism impact**, quantitative criteria have also been used, such as the number of casualties, terrorist attacks, groups or incidents (Jordán Enamorado, 2015). Increased research funding has contributed to the creation, maintenance and enhancement of databases on terrorist events, perpetrators and organizations, marking a noteworthy increase in the number of these quantitative studies. These include American Terrorism Study, Extremist Crime Database, Global Terrorism Database, International Terrorism: Attributes of Terrorist Events (ITERATE), Rand Memorial Institute for the Prevention of Terrorism, Minorities at Risk Organizational Behaviour, Counter Terrorist Trends and Analyses and Maryland University Database (START), among others. The

adequacy of these quantitative criteria to reflect properly the social significance, the predictive value or even simple evaluation of this threat remains contentious in scientific literature as well (Young, 2016), none the less because of definitional discrepancies, methodological difficulties or empirical inaccuracies that render those assessments liable to ideological bias, scientific disciplines' intellectual orientations and self-referential interest of public and private stakeholders, states and parochial constituencies. However contentious these analyses may be, some have pointed out their heuristic value in order to nuance the current European emphasis in terrorism, not only in relation to other geographical areas in the world, but also when compared to OC as to the public resources and expenditure devoted to both threats. Actually, an indirect yet extraordinarily reliable way to infer the relevant social, economic and political impacts of terrorism lies in the post 9/11 overwhelming official response by states and international organisations, i.e., in **counter-terrorism** (CT) strategies, policies and measures, including the EU and its MS. The real effectiveness of CT is in itself an extremely controversial topic that replicates the disordered methodological picture that has been described above as to the usefulness and appropriateness of quantitative (such as averted attacks, arrests or convictions) or qualitative approaches (Cohen/Blanco, 2016), and ultimately their ability to encompass the entire variety of its social and also contested impact. SECILE Project, for instance, accounts for 239 EU CT measures between 2001 and 2013 casting a poor performance in either ex ante or ex post facto assessments, where the societal impacts, including negative impacts on human rights are significantly missing (de Londras/Doody, 2015).

It can be claimed that the EU, its MS and their societies are to a large extent shaped by both OC/TN, but also by the way they are understood and perceived as well as by the extensive and incisive response that has been put in place to counter them. Therefore it is an appropriate starting point to approach those phenomena with a succinct description of the OC/TN landscape in the EU. In this inevitably partial OC/TN mapping in the EU, official accounts (in particular Europol's ones) are given priority because they not only provide a solid –even if incomplete- empirical ground built on national intelligence and LEAs contributions but also because they better reflect the appraisal that underpins the design and content of the EU and MS strategy and policy for responding to those threats.

Terrorism within the EU does not really display a convoluted picture neither in types of terror nor in lethal capacity. This is perfectly in line with quantitative data analyses confirming that over 90 per cent of terrorist attacks are domestic: 'nationals from one country attacking targets of the same nationality in the same country' (LaFree/Yang/Crenshaw, 2010:121) and a similar rate associates terrorist deaths to countries with high levels of state-sponsored terror and to countries that are immersed in some form of conflict whether internal or international. As the 'Global Terrorism Index 2016' concludes: 'This means only 0.5 per cent of terrorist attacks occurred in countries that did not suffer from conflict or political terror [which] underlines the close link between existing conflicts, grievances and political violence with terrorist activity' (IEP, 2016:3).

This is reflected in the relatively simple picture that Europol draws in the TE-SAT 2017 assessment based on 2016 data. Although other four types of terrorism are present in the EU - **left-wing** violent extremism and anarchist terrorism, **ethno-nationalist and separatist** extremism, single-issue terrorism and **right-wing** terrorism - and a consistent number of attacks have been recently carried out (127 fatalities in 2016), the number of reported casualties is extremely low (six victims of paramilitary violence in Northern Ireland and the murder of a UK Member of Parliament) if compared with the outcomes of jihadist terrorism, which killed 135 individuals only in 2016, resulting in jihadist

terrorism as the chief or predominant international terrorist threat within Europe. Although the activity of these other forms of terrorism has risen in recent years, their modi operandi are mostly unchanged (Europol, 2017b), resulting in a highly contrasting picture between the number of attacks, arrests and convictions from jihadist threats compared to other terrorist threats. The true threat thus lies in the persistence of those violent narratives, ideologies and groups susceptible to inspire lone actors (such as the Norwegian Anders Breivik who killed 77 people in 2011) or lure new followers, especially because the internet supplies them a propitious platform for safely spreading their propaganda and indoctrination, fundraising, sharing attack methods or training and accessing to arms and explosive devices or material

Jihadist terrorism has in fact shown the capacity to act and kill across Europe even though the number of casualties per year remains modest in the global context. Although the data show a decrease in casualties in 2016, 135 people were killed and 13 terrorist attacks were reported – the matter stays highly sensitive to the occurrence of a major attack such as those of Madrid in March 2004, London in July 2005, Paris in November 2015 or Nice in July 2016, which killed 192, 52, 130 and 86 people, respectively. Paris in January 2015 (17 deaths), Brussels in March 2016 (32 deaths), Berlin in December 2016 (12 deaths), Stockholm in April 2017 (5 deaths), London in March and May 2017 (6 and 7 deaths) or Manchester in May 2017 (22 deaths) also witnessed significant terrorist attacks with broad repercussions in public opinion. That outcome, which feeds back the efficient jihadist propaganda machinery through the internet and social networks, is also obtained by less lethal attacks with strong symbolic power because of the cruelty or barbarism of the acts such as beheadings or because the victims can be associated with religious and/or western values; hence the targeting of priests, kosher stores, gay clubs, journalists and so on.

Among the variety of jihadist groups and organizations, two are considered paramount: Al-Qaeda and the Islamic State (IS) whose numerous branches and affiliates have spread along the MENA (Middle East and North Africa) area, but also into the Sahel, the Arabian Peninsula and other parts of Africa and Asia, where developing internal or internationalized conflicts and political instability create an environment as prosperous as geopolitically complex. Those organisations at times struggling against each other (e.g. in Afghanistan or Libya) have capitalized this scenario providing the ideological and/or organizational umbrella for jihadist terrorists and groups to act in Europe or against European interests and citizens abroad. Those EU countries that are directly involved in the international coalition against *Daesh* in Syria and Iraq such as France, the UK, Germany and others are singularly targeted by attacks. Indeed, the periodic TE-SAT reports show that the threat is unevenly distributed within the EU.

The intricacy of jihadist terrorism in Europe and how it is presented may be grasped from Europol Director's words: it 'resulted from both unsophisticated lone actors terrorist attacks and well-coordinated, complex attacks by groups of militants. The carefully planned attacks demonstrated the elevated threat to the EU from a fanatic minority, operationally based in the Middle East, combined with a network of people born and raised in the EU, often radicalised within a short space of time, who have proven to be willing and able to act as facilitators and active accomplices in terrorism' (Europol, 2016a:5). The following three points can be mentioned.

(a) Either terrorist lone actors or cells are **largely domestic and/or locally based**; hence the importance of discerning the keen habitats and the paths which lead an ordinary person to become an active terrorist – usually identified as the radicalisation process. The frequent socio-psychological

profile of young Muslim males born and raised in the EU (EU citizens or second-generation immigrants) with low-education level, small chances to prosper socially and economically and petty crime records has experienced many exceptions. Highly educated, women, converts, older men and persons manifesting no external sign of social detachment or grievance sentiment are also in the equation (van Ginkel/Entenmann, 2016)[1]. Previously diagnosed mental problems have been mentioned as well, but it remains a debatable point (Toboso, 2017). This emphasizes the importance of delving into the different narratives that draw people into terrorism and how identity fits in (Neumann, 2016). Degraded neighbourhoods, prisons, families, religious centres or friend circles have been also identified as favourable settings where **radicalisation** may thrive, although truly religious motivations or bonds are not always present and the radicalisation may not take long but speed up to rapid recruitment and action. While much of the *radicalisation* process takes places in these arenas, where individuals may physically find themselves isolated from authorities and services, the process of *recruitment* and connecting with like-minded individuals is greatly expedited by the internet in young individuals' lives. Social media, Youtube, blogs and other platforms serve as the modern dais from which groups such as Daesh disseminate and promulgate their ideologies. They not only act as echo-chambers, reinforcing and legitimising the views of already-radicalised individuals, but allow for messages to be quickly and easily reached by many more vulnerable individuals. 'Amaq News Agency' is a clear example of how these groups utilise these technologies, which produces, publishes and promotes propaganda videos glorifying martyrdom in Syria and Iraq, but which is also accompanied by an assortment of constantly emerging twitter feeds, a twitter hashtag (#amaq), a video channel and an online 'news service'. While most of these emerging associations with the agency are rapidly shut down or censored by most governments, states are engaged in a cyber 'whack-a-mole' with Daesh on this front (Arthur, 2014), where for every one shut down, another takes its place. The ease at which a non-state actor can match a coalition of states in this regard demonstrates the true potential of the **internet** in enabling the recruitment and propaganda function of a terrorist organisation to thrive. However, the simplistic idea of suicidal terrorists should be dismissed, martyrdom coexists with run-away or exit strategies for hiding and hitting again; being both applauded by the official IS mujahidin creed. The absence of internal border checks within the Schengen area enlarges the run-away spectrum (Anis Amri fled Berlin and travelled to Netherlands, Belgium and France before reaching Italy where he was shot down).

(b) The **modus operandi** may be as simple as an attack with knives, small guns and assault rifles (AK 47 appears to have some iconic value) or improvised explosive devices (IED) easily purchased and/or home-manufactured or as unpretentious as using lorries and vans to run over a crowd. But they also may involve more sophisticated warlike modi operandi; hence the importance of **recruitment** and training of the so-called **terrorist foreign fighters**. Some training camps are said to be established on European soil but joining the IS and other terrorist or armed groups in Syria and Iraq through Turkey is considered the most dangerous: 'IS training of recruits consists of imported warfare techniques in the use of weapons, explosives and specific killing techniques, which include beheading. Operatives are also trained in clandestine actions and counter-surveillance. The nature and structure of the training apparently enables IS operatives to execute terrorist acts in an emotionally detached

[1] Spanish-born jihadist Roque (51), married, with four children, former bank employee and gay porn actor apparently became radicalised within a short time while working as informant for German Intelligence service and without anyone in his inner circle realizing (El País, 1.12.2016).

manner, as demonstrated in the shootings in Paris. Acceptance of death is also seen as a facilitator for recruitment and for the execution of IS terrorist attacks. To date there is no conclusive evidence of drugs use playing a significant role in reaching such a mental state' (Europol, 2016b:6). The number of European foreign fighters in Syria remains difficult to establish but the threat merits credit[2]. Following the United Nations Security Council Resolution 2138 (2014), the EU and its MS have engaged in a strong action to outlaw recruitment, transportation and enrolling of foreign fighters, but in dealing with the returned, national policies show quite different approaches, even opposite practices (Marrero-Rocha, 2016). Significant legal measures that have recently been enacted envisage countering this problem, such as the amendment of the Schengen Borders Code Regulation establishing controls on EU citizens leaving the Schengen area, the Directive 2017/541 of 15 March 2017 on combating terrorism (OJ L 88, 30.3.2017) and the Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016).

(c) There is a strong preference by **soft targets** that seem 'more effective than attacks on critical infrastructure, the military, police and other hard targets' (Europol, 2016:6) and do not require large financial requirements often self-provided by the terrorists themselves legally or by means of petty crime. The risk of using CBRN weapons or engaging in high-tech cyber attacks against critical infrastructure remains low. NITs are mostly instrumental for dissemination and propaganda, fundraising and operational purposes. Internet and social media platforms are central in the extremely sophisticated, multi-layered and audience-tailored IS communication strategy. Encryption tools and anonymity services are used to hide locations, protect data and communications or prevent following illicit financial transactions (Europol, 2016a). The financial mechanisms for being able to **fundraise** for a terrorist group vary according to the capabilities of those that seek resources. For example, narratives for financial support to the cause are often encouraged by IS leaders, including Al-Awlaki which in many videos stated 'if you cannot fight you can give money' (AlHayat, 2014). The increase in financial capabilities of terrorist organisations have been seen by Europol, which reported an increment on cyber offences as credit card fraud, PayPal or eBay scams and phishing and hacking (Europol, 2016a: 11). Further changes in the way terrorist organisations finance themselves, in an increasingly modernised theatre, include recommendations to their supporter to misuse government benefits and exploit tax loopholes (Propaganda booklet, 2015), as well as to commit robberies and extort goods and transport –rather than purchase them - such as was the case regarding the lorry used during the Berlin attack, December 2016 (Chazan/Atkins, 2016). This points to the extremely complex issue of nexus between OC and TN that will be analysed later in this report.

Unlike the relatively homogeneous picture of terrorism, **the OC landscape in EU** is extraordinarily diversified and complex. In the analysis of Europol there are five criminal hubs in Europe: (a) North West, with the centre of gravity in the Netherlands and Belgium; (b) North East, with the centre of gravity in Lithuania, Estonia, Latvia and the Russian Federation; (c) South East, with the centre of gravity in Bulgaria, Romania and Greece; (d) Southern, with the centre of gravity in Southern Italy and (e) South West, with the centre of gravity in Spain and Portugal (Europol, 2011a). These hubs are deemed concentrations of illegal logistics which facilitate flows of illicit goods and in which criminal

[2] The EU Counter-Terrorism Coordinator (EUCTC) estimates around 5000 EU citizens having travelled to Syria and Iraq (2016). By February 2016, 3850 names were contained in Europol's Database (EIS). Van Ginkel and Entenmann estimates that the number lies between 3922 and 4294 (2016:3).

groups operate thanks to their proximity to destination markets, commercial and transport infrastructures and major migratory routes. Observing such illegal concentrations, there is a sense that OC is growing **increasingly diverse in its methods, structures and impact on society**. 'A new criminal landscape is emerging, marked increasingly by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors, and aided, in particular, by widespread, illicit use of the Internet' (Europol, 2011a:5).

Criminal groups are also said to expand their activities, with some becoming distinctively poly-commodity in their operations, and with the most successful developing diverse portfolios of criminal business interests (UNODC, 2010). Strong levels of cooperation are detected between different organized groups, transcending national, ethnic and business differences. This 'collaborative atmosphere' is attested by the common practice of barter, whereby illicit goods are exchanged rather than bought and sold, while transactions, it is assumed, tend to jettison the use of cash. A connected tendency is the intensified use of transport infrastructures, with criminal groups taking full advantage of global movements of commodities and growing mobility of people. With the economic crisis, it is felt that OCGs will have new opportunities to recruit disadvantaged individuals, who may find in illicit occupations a ready-made substitute for legitimate work.

These trends seem to be confirmed in subsequent assessments that also emphasize the increasing multifaceted relevance of the **Internet** from big data to virtual currencies and the gradual transformation of OC groups and networks of 'traditional' OC activities (such as drug trafficking or illegal immigration facilitation) into mirroring their peers in cybercrime, which operate 'as part of an online community which is highly dynamic yet fragmented' (Europol, 2015:12). In its most recent SOCTA, Europol stresses this transformation towards a more complex and flexible nature of modern OC networks to the point of deeming obsolete the legal conceptualisation of OC in Framework Decision 2008/841/JHA. Even if most of OCGs are still organised hierarchically, between 30% and 40% of OCGs possess loose network structures and a non-negligible part of them functions on an ad hoc basis, particularly in highly cyber-dependent criminal activities (Europol, 2017a). The general picture is accompanied by a detailed examination of the different sectors of illegal activities (so called **criminal markets and services**) where document fraud, money laundering and online illicit trade are identified as cross-cutting enablers and facilitators of most, if not all, OC endeavours. Money laundering constitutes, of course, a crucial area of investigation, where OC continues to use traditional, established methods such as cash couriers and increasingly post and parcel services (Europol, 2017a), while availing itself of diverse types of shell companies. Moreover, 'Criminal networks continuously seek to exploit the latest technological developments such as cryptocurrencies and anonymous payment methods. Rapid transaction processing and the proliferation of effective anonymisation tools are significant obstacles in the identification of the beneficial owners of criminal proceeds. A growing number of online platforms and applications offer new ways of transferring money and are not always regulated to the same degree as traditional financial service providers' (ibid:18).

Among the criminal markets, drug distribution is regarded as paramount. **Poly-drug trafficking** appears to be increasing, as it ensures greater resilience to fluctuations in supply and demand while maximizing profits (EMCDDA, 2010). At the same time, globalisation and technology accelerates the rate of change in the drug market offering a quick adaptation to new opportunities and opening new ways of distribution, even if drug market-related activities still remain concentrated in some

geographical areas, either established or emerging (EMCDDA/Europol, 2016). Meanwhile, although the majority of **heroin** entering Europe comes from Afghanistan via Turkey and the Balkans, the proliferation of direct transport and commercial links between producing and distributing countries has contributed to diversification in route and trafficking methods. Hence the development of the Black Sea route, which connects Iran, Azerbaijan, Georgia and Ukraine to Romania and the Baltic countries or the Southern route connecting, by sea, Iran or Pakistan to European ports (Rotterdam and Antwerp) across the Arabian Peninsula and East Africa (ibid.). The Balkan route itself shows unprecedented flexibility, as heroin consignments transit through Greece before reaching Bulgaria and Romania and thus Central Europe. The Kosovo region is the operating base of ethnic Albanians involved in trafficking into Central and Western Europe. In the North West hub, Turkish groups are said to be active, along with Dutch and Moroccan organizations, whereas in the North East hub Lithuanian groups service the growing heroin market of the Russian Federation.

Spain and Portugal remain the main European entry points for **cocaine**, which is also imported into the Continent, through West Africa, by Moroccan groups who utilize the North African route established for cannabis. A prominent role in the organization of cocaine trafficking, however, is now taken by West African criminal groups, who hold direct connections with South American producers, standing out Brazil as a key point of departure (Europol, 2017a). Such connections have also been established by groups operating in South East Europe and in the Balkans.

Synthetic drugs offer OCGs the advantage that production may be very close to consumer markets, thus offering a highly cost effective activity. Ecstasy is mainly produced in the Netherlands and Belgium, but tends to be replaced by 'designer drugs' and 'legal highs' such as methylone, mephedrone, fluoroamphetamine and others (EMCDDA, 2010). Synthetic drugs are in high demand in countries where cocaine prices are high, hence the expansion of producing groups, for example, in Poland, Czech Republic and the Baltic States. This ever-innovating drug market appears to be dominated by European producers, resulting in considerable intra-European traffic and exportation to American and Australian markets as well (EMCDDA/Europol, 2016). **Cannabis** and khat distribution complete the information provided by Europol, which singles out West African, Albanian and Lithuanian criminal organizations as the major poly-drug groups. Libya has developed into an alternative route for cannabis resin to enter the EU in addition to the traditional direct entrance from Morocco through the Spanish coast; yet a relevant production of cannabis herb "made in the EU" seems to exist and thrive (EMCDDA 2016).

Illegal immigration is another important area for OC activity, which responds and adapts to changing law enforcement strategies. Although this market reached its peak in 2015, still in 2016 'more than 510,000 illegal border crossings between border-crossing points at the external border of the EU were registered' (Europol 2017:49). Some groups may limit their role to the provision of forged travel documents, while others may offer transport services. Yet others may direct illegal migrants to employers or employ them themselves once they have reached the country of destination. Official reports tended to overlook the instances in which illegal migrants require a mere service helping them move across borders, focusing mainly on the victimization aspect of this illicit business, where obtains **traffic in human beings** (THB) for sexual or labour exploitation – which still remain the main forms for a currently more diversified victim spectrum (UNODC, 2016). For example, 'Traffickers recruit their victims mostly in deprived, disadvantaged or poorly integrated sectors of society, offering them employment abroad. Many victims are lured with bogus offers of legitimate

employment. Others agree on the type of work they are expected to perform, but are deceived by the actual circumstances they find on arrival in the destination country' (Europol, 2011b:10). In the last SOCTA, a clearer differentiation is made between migrant smuggling and THB as two criminal activities that share treating people as a commodity (Europol, 2017a). Of course, the most powerful criminal groups in this area are identified as those capable of controlling the entire trafficking process, from recruitment to transportation, from the provision of forged documents to illegal or criminal employment. The most frequently reported groups involved in human trafficking are, in descending order, Roma, Nigerian, Romanian, Albanian, Russian, Chinese, Hungarian, Bulgarian and Turkish OCGs. Migration flows from North Africa and the Middle East are said to provide criminal groups operating in Europe with opportunities for exploitation, while trafficking is also linked to the commission of welfare benefit fraud, which implies large profits and low levels of perceived risk of detection. Finally, the use on the Internet is associated with the transnational marketing of sex workers.

VAT fraud is a highly lucrative offence. The VAT gap –the difference between expected VAT revenues and VAT actually collected by MS- provides an estimate of revenues lost due to fraud and evasion, tax avoidance, financial insolvencies and miscalculations) has kept steady over EUR 150 billion with the UK, France, Italy and Germany contributing over half of this total (Poniatowski, 2016), while cross-border fraud alone accounts for EUR 50 billion of revenue loss each year according to the recent action plan on VAT of the European Commission (2016). Due to the nature of VAT fraud, which allows numerous traders to exploit the system without affecting each other's profits, organized groups are unlikely to compete in this illicit activity, rather, they most often tend to cooperate by exchanging information and techniques. An attractive alternative to drug trafficking is **cigarette smuggling**, with OC choosing destination countries among those with high taxes on tobacco, such as Scandinavian countries, Germany and the UK, and thus linked in the last SOCTA to excise fraud (Europol, 2017a). In turn, an alternative to the smuggling of genuine cigarettes is the manufacture of counterfeits, whereby well-known brands are illegally produced and marketed, making cigarettes the most frequently seized counterfeit product (ibid.). Poland and some Baltic countries are traditionally singled out as significant sources of counterfeit cigarettes (Europol, 2011a:25).

The **Euro** is yet another target of organised crime (European Central Bank, 2011). Groups engaged in the **counterfeiting** of this currency are characterized by rigid organizational structures and high degrees of division of labour. Participants include investors, printers and distributors, while Italy and Bulgaria are deemed the foremost countries of the activity. Chinese OCGs, instead, are credited with performing a major role in commodity counterfeiting, with goods entering the EU via all major seaports before being distributed throughout the Continent, although some other non-EU countries excel at particular products (such as India for medicines, Egypt for foodstuffs, and Turkey for perfumes and cosmetics) and an intra EU counterfeit OC industry seems to be emerging in order to avoid customs controls and inspections. A joint report of Europol and the Office for Harmonization in the Internal Market (OHIM) describes a highly interconnected multinational cooperative poly-criminal OCG mapping for intellectual property crime and confirms that online markets have become the key distribution channel for counterfeit goods (Europol/OHIM, 2015).

Other areas covered by official reports relate to **weapons trafficking** and **environmental crime**. The former, it is stressed, takes place through the same routes used for drug and human trafficking, and

consists mainly in small or second-hand firearms. The latter implies the dumping of hazardous substances and involves mafia-type structures with sufficient resources to manage the disposal of large-scale waste, although a move towards a more complex business model of illicit waste management seems to exist, where 'illicit waste traffickers now operate along the entire waste processing chain, heavily relying on the use of legal business structures for their activities' (Europol, 2017a:41).

Credit card frauds in Europe are also attributed to organized crime groups, who 'collect data from payment cards by means of attacks on online payment systems, data breaching and skimming (magnetic strip copying and PIN capture)' (Europol, 2011a:23). EMV (Chip and Pin) compliance across Europe has made criminal migrate to overseas jurisdictions for cashing-out and develop deep insert skimmers invisible to the ATM users (Europol, 2016c). Especially when looked at its ever-growing card-not-present (CNP) modality that allows e-commerce fraud, this fraud slips into the cybercrime market: the Darknet and the deep web host a number of sites where plenty of card data are for sale as well as the necessary know-how (Europol, 2017a).

Cybercriminals operates in a global, borderless, extremely flexible quasi-neoliberal criminal market on a Crime-as-a-Service (CaaS) basis opening OC to new 'distributed' models of organization (Wall, 2015). As societies get more and more digitised, cybercrime expands its reach and the digital underworld also open its doors to non-financially motivated actors seeking to make a political stance by defacing a certain website or by intruding networks to access confidential information to release to the public. When is financially oriented, the usually sensitive personal data accessed through a network intrusion can be traded or used for fraud or extortion. Malware development and propagation is key and can be obtained by OC on the Darknet. Stealing information malware such as banking Trojans is well known as is it using ransomware or cryptoware – malware that encrypts information of the victim (or the many victims as the recent 'wanna cry' attack proved) till the ransom is paid usually in cryptocurrencies as bitcoins (Europol, 2017a).

2.2. Organised crime and terrorist networks at the top of the European Union Political Agenda

The landscape summed up in the previous section gives a self-explanatory overview of the importance of tackling both OC and TN at EU and MS levels. This Section expands on how this importance has been internalized into the political agenda focusing on the EU level. More detailed analyses on MS policies and strategies will be addressed in future Working Packages ahead. The legal framework of OC/TN in the EU will be presented first, followed by the examination of how these threats are understood by the EU in terms of security. Some final remarks will be made as to the complexity of current EU institutional framework regarding OC/TN.

2.2.1. General remarks on the OC/TN legal framework within the European Union

Justice and home affairs (JHA) were not among those tasks originally conferred to the European Communities. MS cooperation thus developed using traditional international legal means, either within the more general framework of the Council of Europe or in more specific settings a such as the TREVI Group, the Schengen Agreement or the Prüm Treaty. In 1992 the Maastricht Treaty on the European Union (TEU) brought JHA intergovernmental cooperation to the EU domain under the so-called third pillar whose legal regulation was clearly different from classic Community law and proved overtly inefficient. The Treaty of Amsterdam amended this situation by introducing the **Area of**

Freedom, Security and Justice (AFSJ) as an EU objective and improved the legal regulation of the third pillar, then renamed as Police and Judicial Cooperation in Criminal Matters. Finally, the Treaty of Lisbon eliminated the pillar structure of the EU which replaced and succeeded the European Community, so that the JHA legal regime was finally standardised[3]. This means that every EU action regarding OC/TN must be kept within the **competences conferred** to the EU (i.e. they find a legal basis in the Treaties) and respect the principles of subsidiarity and proportionality (art. 5 TEU) as well as **fundamental rights** (art. 6 TEU). So the general legal framework of OC/TN is determined by those conferred competences that are mainly found in articles 82-89 of the Treaty on the Functioning of the European Union (TFEU) concerning judicial cooperation in criminal matters and police cooperation in order to constitute an AFSJ. Nevertheless, it should be noted that these subject matters are extremely sensitive to MS from a political point of view and several legal caveats have been introduced along the Treaties in order to draw some red lines, such as reminding that national security remains the sole responsibility of MS (art. 4 TEU) or that EU shared competences in the AFSJ 'shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security' (art. 70 TFEU), being the jurisdiction of the Court of Justice limited accordingly (art. 276 TFEU).

Three different areas within the AFSJ[4], upon which competences have been conferred to the EU, are of relevance.

(a) **'Approximation' of MS criminal laws**. The EU can enact directives establishing the minimal rules concerning the definition of criminal offences and sanctions. This soft or minimal harmonisation is limited to those cases of serious crimes with cross-border dimensions. They are specifically mentioned: 'terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime' (art. 83 TFEU). These 'harmonising' directives can also be enacted, should they be essential to ensure the effectiveness of another EU policy implementation, e.g. environmental protection or market abuse. As can be seen, EU law may cover most of the OC/TN landscape, as it actually does – not necessarily in an effective and/or comprehensive way[5]. This baseline report cannot expand on the analysis of all those legal norms, but

[3] This long process has not been done without serious difficulties in obtaining consensus between all the MS. Therefore the AFSJ is still sowed with legal intricacies mostly stemmed from particular legal regimes that apply to some MS (mainly Denmark, United Kingdom and Ireland), the extraordinary variety of the legal instruments still in force and several peculiarities in the decision-making process (Mangas Martín/Liñán Nogueras, 2016). It is opportune to mention that since the Amsterdam Treaty till 1 December 2014, European Commission and EJC's competences for monitoring duly compliance by MS with third pillar measures were harshly restricted. In addition, third pillar decisions and framework decisions lacked and still lack direct effect (former art. 34 TEU). This has resulted in a very defective implementation by MS, as the subsequent mandatory evaluations have confirmed time and again. Their transformation into EU classic norms (regulations, directives and decisions), that the Treaty of Lisbon intended, has been accomplished to a very small extent (Martín-Rodríguez, 2016).

[4] Many other competences conferred to the EU across the TFEU may, of course, be of relevance, since they impact or define the legal substantive framework on which a particular illegal activity of OC/TN develops. Besides the obvious borders' control and migration, Commission's European Agenda on Security mentions transport, finance, customs, education, maritime security policy, information technologies, energy and public health, European Neighbourhood and digital single market (Strasbourg, 28.4.2015, COM (2015) 185 final). This Baseline report cannot expand on those norms.

[5] Regarding the central criminal behaviours, there is the Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime (OJ L 300, 11.11.2008) and the new Directive (EU) 2017/541 of 15 March 2017 on combating terrorism (OJ L 88 of 30.3.2017), which should be transposed by 8 September 2018 and replace Framework Decision 2002/475/JHA (OJ L 164, 22.6.2002). For example, on drug trafficking (Framework Decision 2004/757/JHA, OJ L 335, 11.11.2004); payment fraud (Framework Decision 2001/413/JHA, OJ L 149, 2.6.2001) and euro counterfeiting (Directive

few remarks should be made. This criminal legal approximation is and has proved quite relevant. EU law indeed obliges MS to incriminate some conducts and at least apply a certain degree of sanction (so-called minimum maximum penalties), but it may also involve some important rules regarding jurisdiction and prosecution, the degree of involvement (principal, accessory, aiding and abetting), mitigating and aggravating circumstances or liability of legal persons. Thus the criminal policy of the MS can be profoundly determined by EU law, even though their criminal legal systems remain very disparate among each other. However, these EU directives and framework decisions cannot substitute national law as to comply with the principles of legality and proportionality of criminal offences and penalties, therefore a proper implementation is central to the efficacy of all these norms.

As to the central offences, terrorism and OC, EU harmonising law shows its variety. Unlike international law where no general legal concept of terrorism has been possibly reached, in the aftermath of 9/11 **Framework Decision 2002/475/JHA** was adopted. MS agreed on an extensive incrimination of terrorism based on a broad description of what constitutes the political aims of terrorism (*vs* e.g. OC), a generous list of felonies that, if perpetrated with any of those aims, should be considered terrorist offences and the incrimination of directing or participating in any way in a terrorist group very loosely defined. A third category of terrorist-related offences was later enriched to include terrorism training, recruiting or public promoting. Recent **Directive 2017/541** goes forward in this direction including a new terrorist offence to deal with cyber-terrorism in art. 3 (1) (i) and enlarging terrorism-related offences so as to encompass also receiving training or travelling for terrorism purpose as well as organising or facilitating that travelling in any way. Criminal lawyers have severely criticised this ever-broadening definition of terrorism for a number of legal reasons (Cesoni, 2017). Contrariwise, EU law and international law share the same disagreement as to the definition of OC. Both the UN Convention against Transnational Organized Crime of 2000 ('the Palermo Convention') and the Framework Decision 2008/841/JHA have enshrined the disagreement between common law and civil law systems as to how better pursuing OC – either through a flexible definition of what a criminal organisation is or through the common law conspiracy concept. This defective – actually not even minimum - harmonisation (Mitsilegas, 2009; Obokata 2011) has of course been detrimental to the effective fighting of OC in its own 'pretty' variety, even more when Ms implementations are on the table (Calderoni, 2010). At the same time, the loose definition of what constitutes a criminal organisation or its some remarkable omissions face to the Palermo Convention (e.g. direction) has also deserved a vast criticism of criminal legal doctrine (Calderoni, 2008; Militello, 2015). Truly, OC is characterised by aiming 'to obtain, directly or indirectly, a financial or other material benefit' (art. 1) but, unlike Palermo Convention's legislative guides, no further explanation is made. Europol, on its part, seems to be of an opposite opinion as mentioned earlier in

2014/62/EU, OJ L 151, 21.5.2014); migrant smuggling (Framework Decision 2002/946/JHA, OJ L 328, 5.12.2002) and THB (Directive 2011/36/EU, OJ L 101, 15.4.2011); corruption in the private sector (Framework Decision 2003/568/JHA, OJ L 192, 31.7.2003); cybercrime (Directive 2013/40/EU on attacks against information systems –OJ L 218, 14.8.2013- and Directive 2011/92/EU on child sexual abuse and pornography –OJ L 335, 17.12.2011); environmental crime (Directive 2008/99/EC, OJ L 328, 6.12.2008) or protecting the financial interest of the EU (Convention on the protection of the European Communities' financial interests –OJ C 316, 27.11.1995- and its two Protocols). It is worth mentioning that there is a Commission's Proposal for a Directive on countering money laundering by criminal law (Brussels, 21.12.2016, COM (2016) 826 final) that would supersede the more limited scope of Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (OJ L 182, 5.7.2001). There already exist Directive 2014/42 (OJ L 127, 29.4.2014) and Framework Decision 2005/212/JHA (OJ L 68, 15.3.2005), regarding freezing and confiscation of the proceeds of crime.

this report, calling for an even more flexible definition. Thus, it seems clear that new legislation in this respect is needed.

(b) **Judicial cooperation in criminal matters via mutual recognition**. This EU core competence has drastically changed the landscape of judicial cooperation between MS because this cooperation operates directly between the MS judicial authorities that will execute each other's decisions without the usual governmental interference prevailing on the international legal scene (i.e. mutual legal assistance and extradition). EU **mutual recognition** instruments facilitate a transversal judicial cooperation in criminal matters that is not dependent at all on a previous harmonisation of national criminal or procedural laws due to the **mutual trust** that should prevail among the MS of the EU. This is illustrated by the elimination of the double criminality requirement for a 32 list of criminal conducts when the maximum penalty according to national law surpasses a certain threshold (not very high indeed). The Hague and Tampere Programmes focused on the creation of these mutual recognition instruments, among which the European Arrest Warrant (EAW) stands out[6]. The Court of Justice of the European Union (ECJ) has heavily enhanced the effectiveness of mutual recognition in its case law (Herlin-Karnell, 2013) despite the serious concerns that legal doctrine and conspicuous national courts have manifested as to fundamental rights' protection without any harmonisation whatsoever of procedural guarantees and fundamental rights of suspects, detainees and convicted.

This gap has finally been addressed from the **Stockholm Programme** on and several EU directives have regulated many of these guarantees[7] and, for example, a fundamental rights exception has been admitted for executing a European Investigation Order in criminal matters (EIO). Without denying the substantial improvement on this matter that the Stockholm package means (Mitsilegas, 2016), the contentious relation between mutual recognition, mutual trust and fundamental rights still persists and further ECJ case law developments should not be excluded, maybe driven by the European Court of Human Rights (ECtHR) and/or Constitutional Courts (Martín Rodríguez, 2016). In any case, the problematic functioning of mutual recognition without criminal procedural law harmonisation is still present as legal doctrine has once again showed as to the EIO when there lack common rules on the admissibility of evidence in criminal proceedings (Jimeno Bulnes, 2016; Kusak, 2016). Strengthening judicial cooperation between national judges is the main task of the European agency **Eurojust** (art. 85 TFEU), while a proposal reinforcing its competences is still pending. Conversely, the creation of a European Public Prosecutor's Office (**EPPO**), recently authorised within the European Council[8], would introduce an entirely different approach to judicial cooperation in

[6] After Framework Decision 2002/584/JHA on the EAW (OJ L 190, 18.7.2002), others follow such as Framework Decision 2003/577/JHA on freezing orders and evidence (OJ L 196, 2.8.2003); Framework Decision 2005/214/JHA on financial penalties (OJ L 76, 22.3.2005); Framework Decision 2006/783/JHA on confiscation orders (OJ L 328, 24.11.2006); Framework Decision 2008/978/JHA on the European evidence warrant (OJ L 350, 30.12.2008), repealed by Regulation 2016/95; Framework Decision 2008/947/JHA on probation (OJ L 337, 16.12.2008); Framework Decision 2008/909/JHA on custodial sentences and measures (OJ L 327, 5.12.2008). After the Treaty of Lisbon, Directive 2014/41 on the EIO in criminal matters (OJ L 130, 1.5.2014) stands out, although neither Ireland nor Denmark applies it). It is worth noting the Commission's Proposal of a Regulation on mutual recognition of freezing and confiscation orders, Brussels, 21.12.2016, COM (2016) 819 final.

[7] Directive 2016/1919, on legal aid (OJ L 297, 4.11.2016); Directive 2016/343 on presumption of innocence and the right to be present at the trial (OJ L 65, 11.3.2016); Directive 2016/800 on minor suspects or accused (OJ L 132, 21.5.2016); Directive 2013/48 on the right to a lawyer, to inform a third party and consular assistance (OJ L 294, 6.11.2013); Directive 2012/13, on the right to information (OJ L 142, 1.6.2012); Directive 2010/64 on the right to interpretation and translation (OJ L 280, 26.10.2010).

[8] Council Press release 333/17 (www.consilium.europa.eu/en/press/press-releases/2017/06/08-eppo/).

criminal matters because a European body would be invested with the power to prosecute within the jurisdiction of all MS bound by this 'enhanced cooperation' in order to protect EU financial interests (art. 86 TFEU).

(c) **MS police cooperation**. The EU competences in this field are essentially aimed at information collection, exchange, storage and analysis between LEAs as well as establishing mechanisms and rules promoting operational cooperation between MS LEAs (art. 87 TFEU). This is also the approach of **Europol** – the European law enforcement agency laid down in art. 88 TFEU and Regulation 2016/794 (OJ L 135, 24.5.2016) - as 'a hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services' (Stockholm Programme). So EU action (including Europol) in this field is heavily dependent on reliable information duly gathered and provided in time by MS and the existence of effective information exchange mechanisms on which ground operational cooperation; hence the obligations incumbent upon MS to provide and share information, which are set forth in different legal acts, such as Decision 2005/671/JHA for terrorism (OJ L 253, 29.9.2005)[9]; the establishment of a noteworthy number of EU large-scale database and information systems to be nourished by MS authorities (SIS II, VIS and Eurodac are paramount); and the granting of access to other MS's national databases (**principle of information availability**) where stands out the so called Prüm Decision (Decision 2008/615/JHA, OJ L 210, 6.8.2008) concerning DNA, fingerprints or vehicle registrations. This massive information collection and data exchange, to which the PNR will add when implemented, must be pursued in full respect of fundamental rights, and, in particular, **personal data protection** enshrined in art. 8 of EU Charter of fundamental rights (EUCFR or Charter). This has been quite a controversial issue due to the piecemeal and unsatisfactory state of the play, which was subject to criticism by legal doctrine or the European Data Protection Supervisor (EDPS, 2015) and it led the ECJ to strike down some measures of the Data Retention Directive (*Digital Rights Ireland*, Cases C-293/12 and 594/12; and, more recently, some national data retention regimes in *Tele 2 Sverige*, Cases C-203/15 and 698/15). The recent new legal regime of data protection in Regulation 2016/679 and Directive 2016/680 (OJ L 119, 4.5.2016) is, therefore, a central component of OC/TN legal framework.

(d) **The external dimension of OC/TN EU legal framework**. Given the fact that OC/TN usually work transnationally, the EU and its MS need to establish and strengthen international cooperation with third states and international organisations in order to fighting them more effectively. Therefore, a few remarks should be addressed concerning the external competences of the EU in these fields. After Lisbon, **CJPC external competences** are now governed by the same EU general rules (arts. 216 TFEU) (Eeckhout/López Escudero, 2016). Being EU exclusive external competences unlikely (art. 3.2 TFEU), mixed treaties with third States are also to be expected (Peers, 2016), which means a longer different procedure. Anyway, all these treaties must abide by EU primary law, which has meant that some measures agreed with third countries has been rejected on the ground that fundamental rights are not sufficiently protected in those countries (*Schrems*, Case C-362/14). ECJ's pending Opinion 1/15 on the 2014 EU-Canada PNR Agreement will be crucial. This exemplifies the substantial limits of international cooperation face to the mechanisms, instruments and measures that can be put into action at EU-intra level. It should be noted that this kind of legal issues have already arisen in dealing with particular legal regimes agreed for some EU states (e.g. Denmark access to the new Europol) or

[9] Amended by Framework Decision 2008/919/JHA (OJ L 330, 9.12.2008).

as to the consequences that the exit of the United Kingdom (**Brexit**) may and, to a certain extent, will necessarily unleash ('suboptimal', House of Lords, 2016). An important external dimension has also been recognized to European agencies with Europol, Frontex and Eurojust at the forefront. Finally, it must be recalled that, while EU's external action was deeply rearranged and improved by the Treaty of Lisbon, there remains a harsh legal difference between JHA external action and Common Foreign and Security Policy (**CFSP**) where the Common Security and Defence Policy (**CSDP**) is also legally rooted. As will be seen, this is particularly important, having regard to the securitization of EU understanding of both OC/TN threats, equally active in either external or internal European security strategies.

2.2.2. The general political framework

European Security Strategies reflect the leading role that OC/TN has acquired in both the European political agenda and the underlying securitisation process and architecture. It took a while before a first **European Security Strategy** was adopted in 2003. It was a CFSP document primarily concerned with the changes in the geopolitical international scene and, although rather programmatic and maybe too basic in threat evaluation or in implementation assurances, the EES assumed a broad identification of new threats that may endanger MS security as defined by an overall preservation of European political welfare, values and principles. This approach results in a *security continuum* that is based on an external-internal binary opposition where 'the external menace' (the enemy) puts at risk 'the internal' (the 'us'), which means not only compromising State preservation but also the jeopardy of the rule of law and fundamental rights and liberties (Ruiz-Díaz, 2015). Undoubtedly OC/TN are identified as such external threats of utmost gravity. However, it is to be noticed the self-referential character and the performative effects of securitisation, so it is difficult to discern whether, or to which extent, OC/TN are its main objects or more often than not they have functioned as its most vigorous drivers. Truly this approach with a distinct American accent (the eighties 'war on drugs') has been present for a long time in European countries (it can be detected in the TREVI group) and fostered by the international context and several national milestones from terrorist attacks (e.g. in the Munich Olympic games) to 'mafia'-related incidents (the killing of Italian judges Falcone and Borsellino or the journalist Veronica Guerin). The EU has progressively internalized this security-oriented approach, although admittedly without a prior planning but rather in a disordered dystonic manner reflecting, of course, the evolving legal framework and making use of the increasing EU competences (Bianchi, 2017). With little surprise this approach has taken over the AFSJ objective of the EU and permeated into many others.

Along the past three decades many security-related policy documents such as strategies, agendas, strategic orientations and guidelines, plans of action, joint declarations and so on have been adopted within the EU. Among them, the Renewed Internal Security Strategy and the EU Global Strategy on Foreign and Security Policy deserved some consideration since the European Council defines at the top level the understanding of OC/TN and determines what (goals) and how (priorities) the political framework should engage in.

The important 2010 **Internal Security Strategy** is the first attempt to articulate the whole EU action ('EU's common internal security policy', sic) by defining European internal security and its major threats and setting the model of European internal security, its guiding principles and strategic

guidelines[10]. Four out of the six threats are terrorism, organised crime, cybercrime and cross-border crime. To fight them, a comprehensive approach involving all institutional actors and public and private stakeholders (horizontal dimension) and all political levels (vertical dimension) must be set in order (1) to address not only their root causes (preventive) but also to anticipate those threats through intelligence-led tools and mechanisms; (2) to develop a comprehensive model for information exchange; (3) to strengthen operational and judicial cooperation based on mutual trust and (4) to thicken the external dimension enhancing international cooperation with third states in and outside the EU neighbourhood and introducing security concerns in EU foreign policy and missions. Followed by a Commission's action plan and considered successfully applied[11], this strategy has been renewed by the Council for 2015-2020. The **Renewed Internal Security Strategy** (RISS) – to be read in line with detailed Commission's European Agenda on Security and European Council's Strategic Guidelines for the AFJS[12] - narrows the priorities to terrorism, organised crime and cybercrime[13], but it maintains the same approach of *Europeanization* (internal security is mainly MS's responsibility but there are common threats that must be addressed at the European level to achieve an 'internal security area'); *comprehensive* (in the sense of preventing and intelligence-led anticipating threats, but also enhancing resilience and improving prosecution, an approach that was already present in the **Counter-Terrorism European Strategy**[14]), *multi-agency* and *multi-stakeholders* (with an interesting stress in developing an 'autonomous industrial security policy') and *internally-externally complementary* (envisioning the development of the synergies between EU internal and external action in a much more elaborated way). The implementation of the RISS, which 'represents a comprehensive and realistic shared agenda for the Council, the Commission and the European Parliament', is also enhanced with more concrete goals and actions and a closer monitoring by the Committee on Operational Cooperation on Internal Security (COSI) created by the Treaty of Lisbon. The Juncker Commission itself decisively assumed the priority of this policy 'from day 1' (State of the Union address, 14 September 2016) envisaging the accomplishment of a 'genuine and effective Security Union'. The sizeable, transversal and profound contents that this definitely prioritised policy has achieved in terms of legislative and non-legislative measures can be easily observed by the monthly reports that the Commission delivers.

[10] 'The internal security strategy for the European Union – Towards a European security model', adopted by the Justice and Home Affairs Council at its meeting on 25 and 26 February 2010 (5842/2/10), was approved by the European Council on 25 and 26 March 2010.

[11] European Commission, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22.11.2010, COM (2010) 673 final.

[12] European Commission, European Agenda on security, Strasbourg, 28.4.2015, COM (2015) 185 final) and European Council, Strategic Guidelines for legislative and operational planning in the area of freedom, security and justice according to Article 68 TFEU, Brussels, 26 and 27 June 2014, EUCO 79/14. The RISS was approved by the European Council in 26 June 2015 (EUCO 22/15).

[13] Council of the EU, Conclusions on the Renewed Internal Security Strategy (2015-2020), 9798/15, Brussels, 10.6.2015. These three priorities are: (a) tackling and preventing terrorism, radicalisation to terrorism and recruitment as well as financing related to terrorism, with special attention to the issue of foreign terrorist fighters, reinforced border security through systematic and coordinated checks against the relevant databases based on risk assessment as well as integrating the internal and external aspects of the fight against terrorism; (b) preventing and fighting serious and organised crime, on the basis of the EU policy cycle; and (c) preventing and fighting cybercrime, as well as enhancing cybersecurity.

[14] The EU Counter-Terrorism Strategy (14469/4/05, Brussels, 30.11.2005,) endorses a comprehensive holistic approach to 'prevent, protect, pursue and respond' to terrorism, on which this Report will expand infra.

The **Global Strategy for the EU's Foreign and Security Policy** (EUGS), presented to the European Council by the High Representative in June 2016[15], offers a relevant complementary indicator of the top-rated political importance of OC/TN within the EU agenda as well as the varied dimensions of these threats and the necessary EU counter response. As mentioned earlier the EU external action is still subject to the legal and political cleavage between external EU competences in TFEU and the CFSP, but the international (i.e. also geopolitical) nature of OC/TN obliges to deal with them in a coherent way. These connections have been increasingly present in all the strategic and policy documents along the years and it can now be deemed as a 'political given fact' or as the EUGS apodictically states: 'Internal and external security are ever more intertwined: our security at home depends on peace beyond our borders'. In a more pragmatic representation of its being in the world (Liñán Nogueras, 2017), the EUGS has included terrorism, hybrid threats, cybersecurity and organised crime among the EU challenges where this internal/external interrelation is pressing, singling out counter-terrorism as the ambit more needed of a EU joined-up action. The EUGS displays the numerous ways and instruments that the CFSP/ESDP have at disposal to contribute in fighting OC/TN, stresses the importance of the geopolitical analysis of these threats in doing this when they originate or foster outside EU borders and also confirms that the multi-stakeholders approach and the private-public partnership (especially relevant in cybersecurity) applies. It should be noted that the EUGS endorses the concept of hybrid threats, which 'aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare'[16]. This notion is probably the best example of how OC/TN are moving across fields that were once understood as compartmentalised.

2.2.3. The Complexities of the EU Institutional Framework regarding OC/TN

The Europeanization of threats such as OC and TN has resulted in the progressive establishment and development of a complex institutional architecture at the EU level aiming at operationalizing the European response. This architecture is made of EU institutions and agencies with competence to safeguard internal security and protect the European public order against what are perceived as (mainly) external, transnational threats. The establishment and further development of this institutional framework, however, has neither been entirely peaceful nor a closed chapter after the entry into force of the Lisbon Treaty since many concerns still remain as regards their role in the institutional framework and the coordination of the entire EU response, split into its internal and external dimensions.

AFSJ actors represent a key element of the EU security policy against OC and TN. In the internal security architecture supporting this overall institutional framework, the **Council of the European Union** is the central player. It is guided in the development of its functions by the recommendations and orientations of the **European Council** (art. 68 TFEU), and assisted by different *ad hoc* committees and working parties in its legislative and implementation roles, the most relevant of them being the

[15] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy, Brussels, 28.6.2016, EUCO 26/16.

[16] European Commission and High Representative Joint Communication, Joint Framework on countering hybrid threats – a European Union response, JOIN/2016/018 final, at p. 2.

Standing Committee on operational cooperation on internal security (**COSI**, art. 71 TFEU) – sharing relevance with other somewhat overlapping bodies[17]. Additionally, the Lisbon Treaty has to some extent reinforced the role of the **European Commission** and the **European Parliament** in the implementation and development of the AFSJ, in particular as regards the legislative process (art. 82 and 83 TFEU) and the possibility to bring proceedings for failure (art. 258 TFEU), while maintaining previous restrictions to the powers of the European Court of Justice regarding the AFSJ (art. 276 TFEU).

This internal security architecture is also supported by other AFSJ actors, the **Agencies**. In particular, **Europol** and **Eurojust** assist Member States' LEAs in fighting cross-border threats affecting EU internal security, such as OC and TN. One of the main innovations of the Lisbon Treaty is that the roles of both Europol and Eurojust may be subject to fundamental changes under the provisions of the current Treaties, which endow them with a right of initiating criminal investigations and effective coordination tasks (articles 85 and 88 TFEU), enhancing its operational roles within the EU architecture of internal security – as it has been the case of the last reform of Europol, already in force (OJ L 135, 24.5.2016). Nowadays, Europol's work is supported by special units within its structure in place to fight particular areas of OC and TN, i.e. the **European Cybercrime Centre** (EC3), the **European Migrant Smuggling Centre** (EMSC), and the **European Counter Terrorism Centre** (ECTC), providing the Agency with a pivotal role in the strategic and operational implementation of the AFSJ in its areas of competence. Another central actor within this structure is **Frontex** (currently named **European Border and Coast Guard Agency** (**EBCG**)), whose last reform enhanced its position in the AFSJ and the implementation of its external dimension (OJ L 251, 16.9.2016). To its traditional coordination functions as regards MS joint operations against people smuggling and rapid intervention teams on "hot spots", Frontex added among others tasks competence to assess the capacity and readiness of Member States to face challenges at the external borders (art. 13 of the 2016 Regulation), to adopt urgent measures to ensure the smooth functioning of the Schengen area in case of risks at the external borders (art. 19), to deploy coordinating officers (art. 22) and forced-return escorts (art. 30). As a result of this reform, Frontex has been strengthened as the key actor for the implementation of the **EU Integrated Border Management (IBM**) model at the external borders and implementing EU Law in its fields of competence.

The EU institutional framework is completed with other bodies within the Common Foreign and Security Policy (CFSP) and, in particular, the Common Security and Defence Policy (CSDP) that deserve some attention as they have a say in fighting OC and TN abroad. According to the Treaties, the **High Representative of the Union for Foreign Affairs and Security Policy** shall ensure the coordination and consistency of the EU's overall external action (art. 18 TEU), including thus the policies and instruments having an impact on the fight against OC and TN – namely the restrictive measures against TN and terrorists (art. 215 TFEU) and the activities carried out on the field by CSDP missions and operations against TN and OC. In this respect, the **European External Action Service** (EEAS) supports EU's efforts in countering OC/TN abroad for instance by providing assistance and

[17] COSI coexists with the Article 36 Committee (CATS) and the Strategic Committee on Immigration, Frontiers and Asylum (SCIFA), unlike COSI both tasked with assisting the Council in its legislative initiatives. In addition, the COSI needs to cooperate with the JAI-RELEX Working Party for the external dimension of internal security, and the Political and Security Committee (PSC) for the eventual implementation of the "solidarity clause" (Article 222 TFEU). More information on these bodies at: http://www.consilium.europa.eu/en/council-eu/preparatory-bodies/ (acceded on 25 June 2017).

expertise to third States through EU delegations (where the EEAS has deployed counter-terrorism experts) and support to CSDP missions and operations through its European Union military staff (EUMS) and CSDP-related units.

The main consequence of this complex institutional framework has been, nevertheless, the emergence of an uncoordinated, urgent response at the EU level poorly implemented at the MS level, as well as, indirectly, the expansion of the security measures to the private sector. Firstly, the EU's security policy *strongly relies in the use of* ***criminal law*** – despite lacking a coherent EU criminal policy. In addition to changing the nature of criminal law as a last resort of MS intervention, the criminalization of certain aspects of the activities of OCGs and TN has resulted in other side effects, such as the criminalization of migration (Mitsilegas, 2015), whereas the EU's intervention through criminal law has not favoured the harmonization of MS, as the uneven implementation of the 2008 Framework Decision on combating organized crime has demonstrated (Calderoni, 2010). However, far from being a mere internal aspect of its response, the use of criminal law as another element of EU security policy has been mainstreamed in EU's external policies, providing the basis for the EU to claim being a *normative power* in international relations, as observed particularly as regards candidate countries and neighbouring States encompassed in the **European Neighbourhood Policy**.

Secondly, the complexity of the institutional framework has favoured the proliferation of somewhat **disconnected security strategies**. As noted earlier (Section 2.2.2), during the last decade the Union has successively adopted either general (e.g. European Agenda on Security) or thematic strategies (for instance, EU counter-terrorism strategy) that overlap, and even mutually ignore each other – the more prominent example being the Council and Commission's documents on the external dimension of the AFSJ, adopted in 2005. Even more worrying that this overlap and the vagueness of the wording is the fact that they mostly lack implementation and monitoring mechanisms to assess the results achieved and, if required, to propose further improvements.

Thirdly, the introduction of the AFSJ agencies in the EU institutional framework had as a consequence the **proliferation of 'intelligence' and 'threat assessments'** that guide the response of the Union through the **EU multi-annual policy cycles**. Being the more prominent the Europol's Serious and OC Threat Assessments (SOCTA), the Internet Organised Crime Threat Assessment (IOCTA) and the Terrorism Situation and Trend Report (TE-SAT), other agencies also provide input into the evaluation of the risks to the internal security. This is the case of Frontex Risk Analysis Network Quarterly Reports or the Western Balkans Risk Analysis Network Quarterly Reports, mainly focused on assessing the risks at the external borders as regards people smuggling and trafficking in human beings and drugs. Though biased in their analysis and the collection of data – we need to take into account that these agencies rely on the data provided by national LEAs, these risks assessment reports nurture the EU multi-annual policy cycles to address the main criminal activities of OC/TN, and, thus, the EU response in the various fields of its security action.

Fourthly, the expansion of the EU (legal and institutional) framework has also incorporated the **private sector** in the European response to fight OC/TN. The current legislation, which is due to be completed with other texts under negotiation to reinforce this common response, envisages not only the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004; OJ L 119, 4.5.2016), but also *inter alia* the obligation of the banking and finance sector, external auditors, notaries, estate agents and providers of gambling services to provide **competent national authorities and Financial**

Intelligence Units (FIUs) relevant information to fight money laundering and the financing of terrorism (OJ L 141, 5.6.2015).

Further expanding on the complexity of the EU institutional framework, however, goes beyond the scope of this baseline report. Subsequent TAKEDOWN project deliverables will deal again with this complexity and provide some recommendations for first-line practitioners and professionals.

3. Organised Crime and Terrorist Networks in Scientific Literature: Revealing the Layers of Complexity

TAKEDOWN Project seeks to develop effective and efficient security solutions for first-line practitioners and professionals in identifying, approaching and responding to organised crime and terrorist networks. It accordingly focuses in better understanding the social, psychological, economic and cultural aspects that leads to OC/TN in a way to improve cooperation between the stakeholders involved in preventing and responding to these threats as well as to inform policy makers on the better practices and strategies. Thus TAKEDOWN project has reviewed scientific literature on OC/TN with a very specific purpose which is providing with a solid scientific background for the following tasks and particularly the model design set out in Task Force 4 (Ruggiero/Leyva, 2016). This review has allowed screening those models employed in scientific literature in order to assess their suitability for the project highlighting their core methodological challenges in Deliverable 2.2. This Baseline Report is thus the result of both operations (reviewing and screening), but it does not intend to summarize them up but showing instead their main achievements and conclusions. The core claim, as will be seen, is that advances in scientific knowledge have not end up in a more precise delimitation of both OC/TN but quite the opposite: the chief contribution has been to reveal their **extraordinary complexity in terms of causes, structures and activities** and, consequently, in the vast array of the measures, tools and policies that countering them demands. This last point is of particular importance for TAKEDOWN project which is, as mentioned earlier, first line practitioners oriented.

This complexity revealed by academic and research literature may be displayed through four different strands that somehow show certain variations in scientific focus and priorities, but without fully abandoning or rebutting previous findings, acting more like a cumulative collective endeavour, such as moving from deterministic causal ambitions to process explanations, the increasing analytical *acquis* stemming from different scientific disciplines that focus on concrete dimensions, stages, functions or activities and cast an undisputedly multi-dimensional and multi-faceted global depiction, the increasing knowledge regarding the nexus between both OC/TN and, finally, the crucial repercussion of new technologies and internet. Notwithstanding, with regard to this scientific contribution two previous general remarks that criminological studies may illustrate are submitted here. First, there is a **persistent empirical caveat** despite the gigantic volume of research projects, studies, articles and official reports devoted to OC and TN (Silke, 2008). This caveat is possibly unsolvable since it is not only related to the scientific credentials of some qualitative methods usually applied (Freilich/Chermak/Gruenewald, 2015 as to TN) but also to the reliability and accuracy of the empirical data that quantitative methods work with[18]. A consequence thereof has been a notable **self-awareness and self-reflexive** feature in criminological studies that acknowledge these empirical limits and in a way also accept the pertinence of critical studies dealing with the socio-political – and scientific too- construction of both OC/TN (Mann, 2014)[19]. Secondly, OC/TN criminological studies

[18] Keeping its first-line practitioners-oriented perspective, TAKEDOWN project will address this insufficiency in Task force 3 including a quantitative survey as well as qualitative approaches such as expert interviews, workshops and focus groups.

[19] In her extraordinary Ph.D, Mann traces how the different OC conceptualisations that have prevailed in criminology literature are linked to the intellectual climates at the time. Criminology operates as 'regime of truth' in a Foucaultian sense, legitimising the emergence of the social problem of OC, which is constructed within an interconnected set of four social, political, moral and bureaucratic discourses (law and order, new management in policing, securitization and wars on

also illustrate the openness towards other academic disciplines showing an increasing although not unproblematic (von Lampe, 2006) **interdisciplinary component** especially coming of course from economics but also psychology, anthropology and political science.

3.1. From causes to processes

The interpretation of the causes of organized crime shows an extraordinary continuity in time. For over a century its aetiology has been based on categories such as tradition (Lombroso, 1971), absence of the state (Gambetta, 1992; Edwards/Levi, 2008), pathology (low self-control – Gottfredson/Hirschi, 1990) and lack or decline in informal social control (social disorganization – Downes/Rock, 1988), relative poverty, and delinquent subcultures (Coheh, 1955, Clowar/Ohlin, 1960), pushing individuals to resort to illegal activities – innovate - in order to solve their status problems (Merton, 1968) or substituting the state through a surrogate social system (Landesco, 1969) or a type of governance (Varese, 2010a). All these categories fall, to different degrees, within a **paradigm of deficit** whereby the causes of crime originate in a deficiency, be it one of control, of socialization, of opportunities, of rationality, and so on (Ruggiero, 1996). A slightly different perspective, but extraordinary influential on the explanation of OC, is hold by those who understand that those groups are actually illegal enterprises (Block, 1991; Becker, 1968, Andreano/Sigfried, 1980), hence OC should be approached as an economic activity. Contemporary structural perspectives hold the same reasoning pointing that the neoliberal globalisation has generated the conditions for criminal opportunities to emerge (Chin/Godson, 2006; Ferreira, 2016; Mazzitelli, 2007; Tzvetkova, 2008; Wang, 2013) because of the increasing socioeconomic and political inequalities, the weakening of state regulations and the decline in public services. This vast array of causes suggested by literature reflects in a **multi-dimensional factorial portrait** disclosing their interaction and allocation along the macro, micro and meso levels (Figure 1).

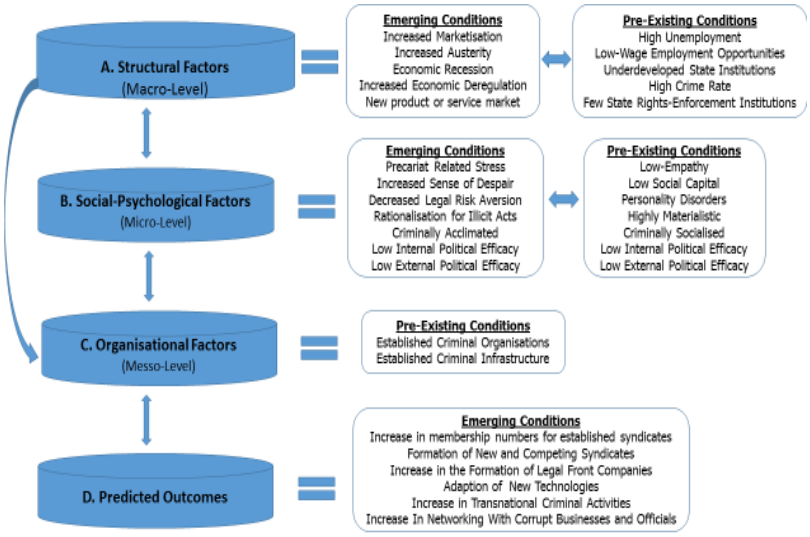


Figure 1. Multidimensional model of organised crime. Source: Ruggiero (2016): TAKEDOWN Deliverable 2.1

crime and forging the outlaw identities) that provide the impetus for the institutionalization of the phenomenon in a mutually reinforcing and complex process, since it justifies the expansion and hybridization of new intelligence and enforcement agencies, whose activities and operation confirm OC as a serious problem warranting intervention, and the continued funding of these very agencies themselves (2014).

Criminology studies have approached terrorism as a manifestation of the more general category of **political violence**. Some classical authors linked thus political violence by either individuals or the state, as a breach of social contract (Beccaria, 1965; Bentham, 1967). Some others however found a difference between revolution and rebellion, the latter being caused by insanity, moral madness narcissistic martyrdom or suicidal drive (Lombroso, 1984). In Durkheim studies it may be the result of excessive integration in a creed or an identity (1996).

Terrorist acts as form of intimidation of political opponents appear as a component of collective conflicts in the struggle for attainment of material and ideological power (Landesco, 1969), whereas within violent conflicts terrorism seems a an indiscriminate confronting method justified by abstract representativeness of the other party and of course its efficiency, particularly in asymmetrical conflicts. In its manifestation as 'pure violence', terrorism retains some elements of so-called hate crimes that, if applied reciprocally, can rapidly become war-like (Witte, 1996; Black, 2004; Ruggiero, 2005).

Severe social inequality and injustice – somewhat counter-intuitively - is not necessarily linked to terrorism (Laqueur, 2002). While theology studies are controversial as to Islam religion causing terrorism (Kennedy, 2016; Small, 2016 vs. Horkuc, 2009; Wills, 2016), others point to the fact that religion in general has always played a role in war and terrorist violence, even in advanced secular countries (Buc, 2015; Sacks, 2015; Hassner, 2016). Ross (1993) suggested a general causation model for oppositional political terrorism that tried to capture, through various propositions, the intricacies and intertwines of all relevant structural factors (permissive and precipitant causes) (Figure 2, below).

Contemporary debate has abandoned the notion of the roots of terrorism – seen as a somehow justificatory - taking instead the concept of radicalisation (Neumann, 2013). Being **radicalisation** different from radical political thought, violent extremism and ultimately terrorism (Dzhekova et al, 2016), the fact that this concept, broader and narrower at the same time, has drawn and framed the discussion on the root causes of terrorism seems to say 'more about the speakers and their governments' ideologies than about the terrorists' intentions and motivations' (Schmid, 2013:2).

Underlying thought seems to be the politically and socially widespread idea that radicalisation would capture the very 'efficient cause' of terrorism as much as this simplification barely holds (Dzhekova et al, 2016). However, this might only move the point one step further as to what are the root causes of radicalisation leading to terrorism and here again, within the radicalisation debate, this causation re-emerges in full variety looking at the different levels where these factors lie in order also to enclose the individual dimension (see, e.g., Velhuis/Staun's categorisation (2009) in Table 1).

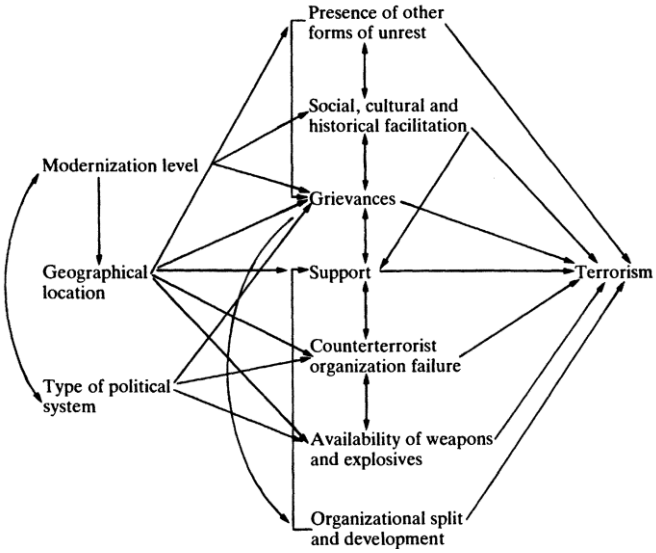


Figure 2. The general pattern of causation among the structural causes of oppositional political terrorism. Source: Ross (1993)

	Types of causes*		*Types of catalysts**
Macro level		Political Economic Cultural	Trigger Events
Micro level	Social	Social identification Social interaction & group processes Relative deprivation	Recruitment Trigger Events
	Individual	Individual Psychological characteristics Personal experiences	Recruitment Trigger Events

** The factors in the model illustrate the type of causal factors categorised at each level, and can be complemented and extended by related factors.*

Table 1. Categorization of causal factors of radicalisation. Source: Veldhuis/Staun (2009)

These causes' review reflects – and in a way tries to dodge - the underlying issue of the social construction of these concepts. They are used, as von Lampe has stated regarding OC, as if they denoted clear and coherent phenomena, while they are in fact ever-changing, contradictory and diffuse constructs bringing together a multiverse of social realities that only makes unified sense on the linguistic and cognitive level (2008). The underlying disagreement or, if you like, this social construction emerges time and again when defining what terrorism or organised crime really are. Their varied international legal definitions depending on the facet that is envisioned by the legislator, or their absence as mentioned earlier, are but a conspicuous example. However, from the point of view of TAKEDOWN project, this situation is relevant in the four different senses that follow.

(a) *The **social construction** of these concepts brings the need to know which myriad of social realities they try to encompass in order to identify their natures, dimensions, structures and so on, and*

consequently the reach which their explaining models may ambition. This point may be illustrated by the dissection made by von Lampe mentioned earlier showing that OC encompasses at least these three strands:

> 'One view holds that organised crime is primarily about "crime". Organised crime, therefore, is seen as a *specific type of criminal activity* characterized, for example, by a certain level of sophistication, continuity and rationality in contrast to sporadic and impulsive criminal behaviour. According to another view the emphasis is on 'organised'. It is not so important what offenders do, but *how they are linked to each other*. Organised crime, therefore, is about some form of criminal organisation in contrast to lone offenders. Finally, there is a view that organised crime does not have to do primarily with specific forms of criminal activities or specific collective forms of crime, but with the concentration of power, either in the form of an underworld government and/or in the form of an alliance between criminals and political and economic elites. From this perspective organised crime denotes a *systemic condition*' (2008, italics added).

It is clear that each of these three strands opens an entire different (though non-mutually exclusive) avenue of research and analysis that are actually pertinent, but also able to evolve in their own right. For example, the **systemic approach** emphasizes the 'necessary embeddedness of organised crime in society' (corroborated along the history of OC – Fijnaut/Paoli, 2004:229) and the OC need to establish meaningful external relations with it, which in turn is crucial to understand the causes (Scarpinato, 2004; Dino/Pepino, 2008) but also the successive stages (predatory, parasitic and eventually, symbiotic) that OC may experience (Peterson, 1991), even identifying a 'mafia method' as a series of principles, modalities and values that mutually spread from criminal organizations throughout the official world and vice versa, affecting the concepts of justice, morality and enterprise (Dino/Ruggiero, 2012).

(b) *The social construction of these notions makes them **sensitive** to the **interest and perspectives** of the **different stakeholders involved*** – in order to gain consensus, resources and domestic powers increase (Carrapico, 2014). Europol accounts, as most LEAs' ones, have successively moved, for example, from focusing from mapping groups (OC hubs) towards the identification of 'criminal markets', mostly analysed by describing the criminal conduct and some traits of the modus operandi and implicitly assuming the seriousness paradigm (Sergi, 2015). The threat assessment, key to the policy cycle featuring the move from OCTA to SOCTA has been deemed to imply and unleash very specific consequences in the social shaping and intellectual understanding of these phenomena as well (Edwards, 2016). *Hence the social shaping of these concepts must include the **repercussions of countering measures, policies and strategies** in order to avoid precisely counterproductive results*. As mentioned, terrorism is not homogenous in Europe, but the media and the political agenda has shifted excessively towards jihadist terrorism. The elevation of this form of terrorism to threat-number-1 against the West is one of the elements that instigates separation and alienation among the Muslim community and the rest of society. It should be kept in mind that many other forms of violent extremism have emerged such as right-wing or left-wing extremism. These forms, however, feed off one another to create a more complex interaction between violent groups and the state, with each group and type of violent extremism requiring different policies, solutions and responses.

(c) *The vast array of causes should be reflected in an **enlarged countering and preventing measures' approach**, involving many different stakeholders and also keeping in mind the numerous public services that become relevant for tackling OC/TN*. This multi-stakeholder approach, on which we expand below, holds not only for a 'structural' prevention scheme, but also for 'operational'

prevention purposes (terminology borrowed from the Report on preventing deadly conflict – Carnegie Commission, 1997).

(d) ***Epistemologically***, it can be assumed that despite the undeniable relevance of this research on the causes, the idea of finding causal or deterministic models is rather futile and ***analytical models*** depicting these processes instead should be pursued (von Lampe: 2003). However, the most relevant issue, at this stage of the Report, is to note that *the social construction of these notions and the variety of realities that they conveys makes most of the research approaches (and many of the **models** deduced from them)* ***partial*** **per se**. Hence the need to build upon that body of literature with the objective of cumulatively enlightening the varied dimensions of OC/TN and the models used to delve into them more than finding the one. This is expanded in the following section.

3.2. Towards a Multi-Dimensional Understanding of Organised Crime and Terrorist Networks

The volume of research and publications that have studied and analysed a relevant dimension of OC/TN is monumental and it would be impossible to summarise even vaguely all the pertinent insights that can be deduced from that gigantic body of research. **Particularly powerful criminal and terrorist organisations** (ranging from drugs cartels, Mafia-organisations of most diverse ethnicities to Al-Qaeda, Hezbollah or Daesh) have vigorously drawn the attention of researchers, investigators, journalists and many others because of their international reach and impact, their luring secrecy and power, the virulence of their methods or their geographical salience. **Specific illegal markets** (all types of drugs, human trafficking, arms trafficking, extortion and protection racketeering, etcetera) as well have been studied **at the international, national or local levels**. Those analyses reproduce the multi-dimensional character of these processes.

An important strand have also analysed aspects or variables intrinsically linked to OC such **violence** contradicting common clichés. Violence is mainly a subsidiary regulatory mechanism (more than an individual propensity) and its appearance is an indication that something has gone wrong in the milieu and not a common or systemic feature of any organized crime setting (Morselli/Gabor/Kiedrowski, 2010). Trust and the collaboration of experts are other topics of relevance. However, utmost attention deserve **corruption** and the **reinvestment of the OC proceeds in legal business** with which OC assures endurance by penetrating the legal economy and the public authority system (Iacolino Report, 2013). So emerges the key **legal-illegal continuum**. Gounev and Bezlov (2010) make an extensive study on the relations between OC and corruption through a meticulous literature review and a mapping of corruption in EU MS through different statistic data with respect to public bodies (ranging from politicians to the judiciary) and the private sector. Among their interesting key findings these two are: corruption is rarely associated with OC, since 'white collar crimes' are commonly seen as distinct from OC; the relationship between corruption and OC in some MS (E17) is mainly confined to 'white collar crimes', whilst in the 10 other members it has resulted in a fusion of the underworld and the 'elite' (ibid.:149-150). According to a recent report (D'Angelo/Musumeci, 2016), the penetration of OC into the legal economy in Italy is operated through creating monopoles, illegally accessing to public biddings or taking control of legal enterprises – particularly those with strong cash-flow as real state, gambling, and others that facilitate money-laundering or subsequent commissioning of OC illegal activities -, and it counts with 'collaborative' (collusive) private sector actors and professionals as well as corrupted politicians,

ending in the continuum mentioned above. The modus operandi of this penetrations is represented in a theoretical model in Figure 3 below.

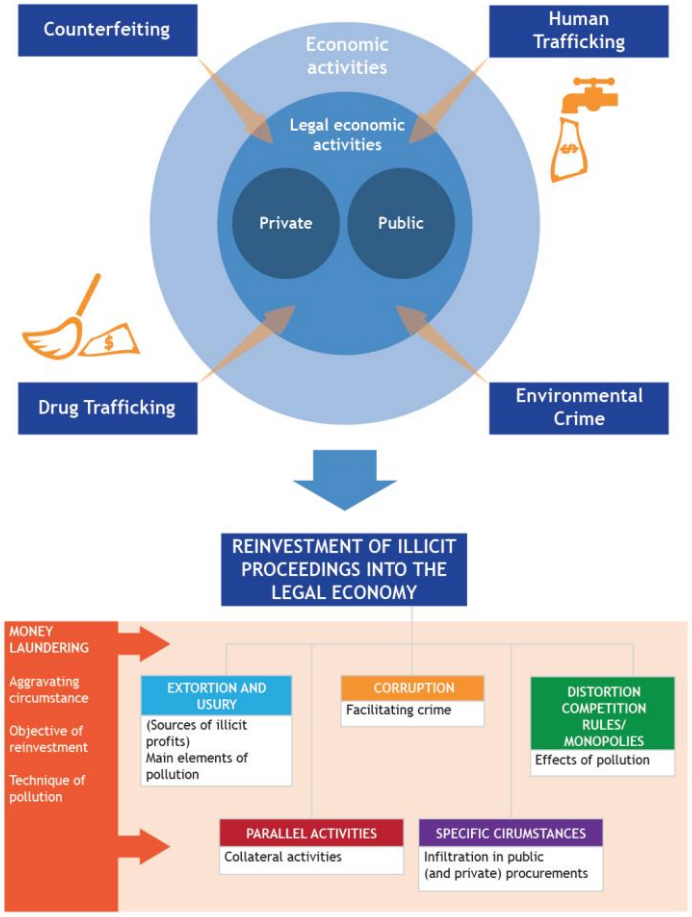


Figure 3. OC penetration in legal economy - theoretical model of the modus operandi. Source: D'Angelo/Musumeci (2016)

Again, literature has accrued the knowledge field on OC/TN focusing on different dimensions whose utility for understanding OC/TN is not only theoretical but may well be translated into more practical uses. For example, gender is an interesting variable to look at, since the notion that both OC/TN are fundamentally male phenomena has been long proved inaccurate. Beare, for example, focuses on OC in Canada and offers a picture of the offender type, their more frequent roles in certain OC activities, their attitude face to violence and so on; showing that the positioning of women within OC organisations is more significant than thought: even if leading positions are uncommon, they play relevant trustworthy managerial roles (Beare, 2010). Several of those points are confirmed in other studies that highlight frequent family or partners bonds explaining the relevance that gender has in internal OC dynamics, including trust – internal security - (Requena et al., 2014) and in terrorist networks (González/Freilich/Chermak, 2014). On a more critical note, gender studies might also illustrate the nature of OC as structurally reflecting, construing and perpetuating heterosexual male domination (Núñez-Noriega/Espinoza-Cid, 2017).

These impressive amount of information is, naturally, of relevance since beyond the need for more general theoretical analyses, the only trait remains that each OC or terrorist group is unique in its manifestations. For that reason, TAKEDOWN Project will complete this Baseline report with an **open hub of information**, where these sources are identified and classified, particularly emphasising when

they are available or open to public access. In the following this section will only review some aspects that are deemed of relevance.

One of the most debated issues in literature is, of course, to find models capturing the **nature** of OC/TN, in particular because their manifestations show a rich variety of types that researchers and authors have – admittedly, strongly influenced by their own ideological affinities and scientific conceptualisations, notably of OC - tried to classify and categorise. While this question is particularly complex in OC, terrorism seem to be treated as something more monolithic in its nature, whence based on that assumption the focus of 'modelling' literature has been conveyed to the internal structures: whether a hierarchy, a cell network or a combination of both. This would make some of the models designed for understanding OC unsuitable for TN, due to its different non-profit-seeking nature. The emergence of nexus between OC and TN makes though this idea less compelling and therefore OC models might be pertinent for TN at least in this nexus hypothesis (see below). The difficult task when modelling OC is to encompass the variety of groups that current OC shows and common legal definitions endorse with the powerful realities of traditional Mafia in Italy or the mythic force that the conspiracy of Italian migrants 'crime families' alien to the US society (Kefauver Committee, 1951; Cressey, 1969; Ianni, 1972; Fijnaut, 1990).

It should be recalled that, according to art. 2 of the Palermo Convention, an 'organized criminal group' requires 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 in order to obtain, directly or indirectly, a financial or other material benefit. Specifically, legal definition excludes the need of formally defined roles for its members, continuity of its membership or a developed structure. Illegal enterprise becomes key and the elements of specialization and hierarchy present in classic OC definitions are dropped without that meaning that hierarchical and specialized organizations disappear, making crucial to draw the distinction between producers of goods and services, and suppliers of forms of regulation, protection and governance (Varese, 2011). The form of governance alluded to is one that usurps the functions of the state in societies where sovereign rule is inadequate, a form of governance from below which extends power 'beyond the state and into the realms of civil society' (Edwards/Levi, 2008: 379). From an entrepreneurial view OC would then be an industry for the supply of private protection and the distribution of trust to economic actors who would otherwise be unable to interact safely (Gambetta, 1992).

When defining the nature of these structures, Albanese (2011), for example, suggests differentiating three types of OC:

> (a) the ***hierarchical model*** is found in traditional 'Mafia' organised crime structures and the more traditional terrorist groups, such as the IRA. The groups are organised according to a top-down leadership hierarchy with one person (or controlling group) on top of pyramidal structure and many soldiers at the lower levels with a number of levels of authority in between the levels.
>
> (b) The ***ethnic-cultural model*** shares a common heritage that engages in both low-level and high-level crime to the benefit the entire group. Ethnic, cultural or religious ties bind the group together and individuals mostly control their own activities to achieve a common goal which may be criminal or terror oriented. They (ethnic, cultural or religious ties) create trust and bond "organised criminals" together (von Lampe/Johansen, 2004). This trust bond helps the resulting networks to reduce uncertainty in a field where there cannot be law enforcement intervention. It also gives to its members a competitive advantage in business, thanks to the

tight social relations. Trust plays an important role from the point of view of collective action (Paoli, 2002), because it is a strong non-economic tie which allows these groups to be better organised than any other social group.

(c) The ***entrepreneurial model***, contrasts with the hierarchical and ethnic/cultural models, mainly because the organised crime groups operate more like legitimate business enterprises, but focus upon illicit instead of legitimate markets to provide illicit services and/or goods. They are rarely organised in a centrally coherent way, rather they operate like businesses along the similar principles that govern legal markets in order to maintain and extend their particular share of the illicit market, responding to the needs and demand of their consumers. The aims of the groups falling within the organised crime enterprise model are mainly profit, rather than ideology, driven, however, such profit could be used to fund a terror campaign. Regardless of whether the goal is organised crime or terror, illegal and expanding markets still require a high demand for protection of property rights where the State and the law cannot help. So, there might be the need for an alternative instrument of protection and in such a case, the formation of Cartels, groups of actors who agree to control prices, are an efficient way of excluding newcomers from the markets and insure that profits will be equally shared (see later discussion).

Edwards (2016) calls the attention to the actor-oriented perspective that all these three models share suggesting instead a different approach focusing on the **commissioning process** – how serious criminal activities are in fact 'organised' through criminal scripts, scenes and scenarios - and the identification of its vulnerabilities as a more solid ground where deducing effective harm-reduction policy priorities (see Table 2, below). A similar distinction is used by Ruggiero (2016) as a better approach to apprehend the structural implications of the legal-illegal nexus: instead of an association formed by culturally or geographically homogeneous group of individuals – crime in association, OC substantiates a series of transactions between individuals involved in a common activity irrespective of their social and cultural background – crime in organisation. From this perspective visibly emerge the links that the criminal group establish with external, mainly official actors with whom joint activities are carried out (Arlacchi, 1983, 1994; Armao, 2000; Lodato/Scarpinato, 2008; Gounev/Ruggiero, 2012).

The alliances and partnerships between organized crime, the official economy and the political world suggest that organized crime combines forms of conventional criminality with a variety of white-collar offences. This happens when proceeds from illicit activities are invested in the official economy, where members of criminal groups 'learn' the techniques and the rationalizations of their white-collar counterparts. In this case, it is appropriate to talk about a number of exchanges and a mutual entrepreneurial promotion in which the different actors engage. Hence, he claims that we currently face these criminal networks more than properly criminal organisations (Ruggiero, 2016).

Trend	Analytical Focus	Policy Exemplars
The Actor-Orientation (1): Conspirators	Organised Crime Groups (OCGs)	Kefauver Committee (1950); US Presidential Commissions on OC (1967, 1986); RICO statute (1970)
The Actor-Orientation (2): Illegal Entrepreneurs	Illicit networks	German BKA\LKA definition of OC (1986)
The Actor-Orientation (3): Poly-Criminals	'Potpourri' of 'threat indicators': OCGs SOCs (Serious Organised Crime areas) CRFs (Crime Relevant Factors) Effects of OCGs + SOCs on EU society	UN Convention Against Transnational Organised Crime (2000); Annual EU Organised Crime Threat Assessment (2006-2011); EU Serious and Organised Crime Threat Assessment (2013 – 2017)
Organisation of Serious Crimes: Commissioning	Scripts, Scenes and Scenarios	Approach still marginal and primarily based in the academy, e.g. RUSI (Royal United Services Institute) Organised Crime Programme (2014)

Table 2. Organized crime policy trends and their analytical focus. Source: Edwards (2016)

Unlike the OC complex picture, terrorist groups apparently seem to offer a simpler image with a transition from highly hierarchical to **looser networked structures**. Truly, when there is popular support because the terrorist groups maintain strong links with social movements and are perceived as representatives of the aggrieved, a dual structure might appear with a core of hidden clandestine combatants and a wider, official, legitimate layer of activists (Combs, 2013; Martin, 2010). The loss of that social connection may end up in the collapse of the terrorist groups (Ruggiero, 2010a). But concerning the internal structure terrorist groups in the 1990s tended to have a high degree of professionalism and role differentiation, a clear pyramidal command structure and a selective recruitment based on proven ideological loyalty, military expertise, resource possession and social capital. The central committee decided the functional structure as well as the political long-term and short-term strategy. This structure has been replaced by the creation of cellular units more or less coordinated and with weaker links to the central core. Attacks from scattered cells follow thus more a logic than a programme, 'revolving around the symbolic nature of the destructive act, a form of signature indicating a common identity' (Ruggiero, 2016). This cell-networked structure continues to be the dominant trend, although the central core sustains, nurtures and defines the 'terror mission', articulates its crucial propaganda and publicity across the cyberspace and social networks, claims responsibility and authorship of disseminated cells' and lone actors' actions and so on, in what has been called 'global terrorism'.

The literature has emphasised those cases when the central structure is not only geographically located (which is usual) but actually wields military power and engages in open conflict, such as ISIS, Al-Qaida and others. This central node is accrued through the recruitment and enrolling of former jihadists, professional soldiers and intelligence personnel (Whiteside, 2016) commanded by a vertical apparatus and functional bureaus. Thus, along with hierarchical organizations, there are bands of followers who act outside formal structures but motivated by feelings and beliefs widely shared within the world Muslim community (Blum/Heymann, 2010). These cells coexist with unstructured home-grown counterparts lacking leadership and links with the external organisations (Vidino, 2011)

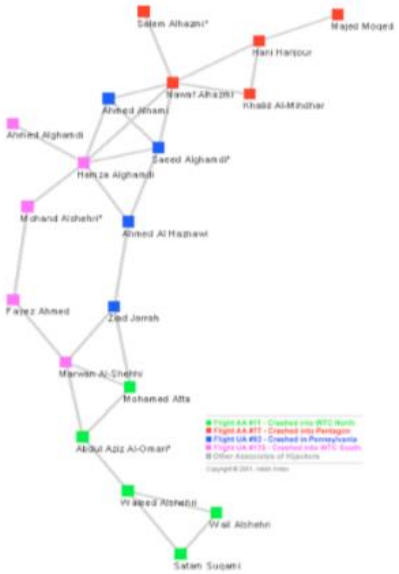
in an outstandingly uneven landscape across EU countries (Dzhekova et al., 2016). Outside the network lone-actors pose clear difficulties in detection and disruption since they act in isolation, without guidance, communications or potentially any interaction with a wider group. However 'it is not always clear that lone actors are truly alone, and usually investigation uncovers contacts, leakage and evidence of connection with others that casts doubt on the degree of isolation that can be attributed to an individual' (Pantucci/Ellis/Chaplais, 2015:1) or to what extent lone action is the result of a failed integration within the radical milieu (Spaaij, 2010).

Right-wing extremism structures instead are extremely varied and seem impervious to general modelling and better explained through social movement approaches. Ramalingam mentions informal groups and networks, such as youth gangs, white power and skinhead groups, sports and music groups, terrorist cells and lone actors, political movements and paramilitary groups; and nativist and anti-Islam movements, but also political parties and other electoral organisations (2014). Despite the facts that the low-intensity and dispersed nature of the violent behaviour showed (with notorious abominable exceptions) could make feel inclined to downgrade their heterogeneous manifestations and, admittedly, right-wing extremism poses a major challenge for identifying the thresholds between radical thought, violent actions (hate crimes) and terrorist activity (Ramalingam, 2012) – whereby radicalisation looks the appropriate framework -, their embeddedness within society and particularly their insertion into the political system thanks to a layered calculated ambiguousness towards democracy and constitutionalism should raise concern about this crucial difference face to jihadist terrorism. OC insights on the **legality-illegality continuum** might well prove useful in disentangling these structures.

A portion of the 'modelling' literature focuses on the internal structure of organised crime groups and terrorist networks. It tries to explain what bonds a group of criminals together and how the group and single members behave under specific requirements. Polo (1995) developed a **competition model**, concentrating on the internal structure of the Mafia, using a principal-agent approach, which is based on trust and wages. In such a model, the boss pays a specific wage to his soldiers and according to that level they decide to be part of the organisation or to leave the organisation. Baccara and Bar-Isaac consider 'the trade-off between the increased internal cohesion derived by exchanging internal information and the increase in vulnerability to detection that this exchange implies' (Baccara/Bar-Isaac, 2008:3). Since secrecy is vital for the survival of the organisation, information flow is strictly limited. Therefore if a peripheral member were detected, it would not undermine the entire group because the information at his or her disposal is limited. Accordingly, two detection strategies could be implemented to tackle an illicit organised crime group. In the ***agent-based detection model*** there is an authority that focuses on each agent independently and success depends only upon that agent. In contrast, the ***cooperation-based detection model*** relies upon co-working: 'in which the probability of detection is an increasing function of the cooperation level of the agents' (ibid.:32). These two detection models are actually a reversal of what happens in Terrorist Network groups (Krebs, 2002) and particularly in the early phase of the recruitment process (Berry et al., 2004).

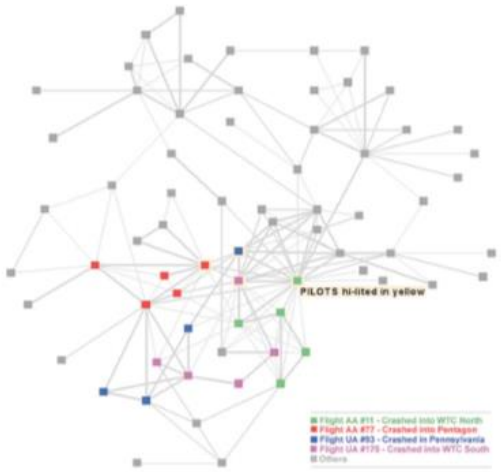
Network structure has logically been the object of deep analyses. As seen, OC and TN seem both moved towards more loose structures and functioning although it does not mean that more hierarchical components or groups yet exist, co-exist or combined with them. This is of course present in OC literature that has shown some decline in the use of the organization theory in favour of network analysis (today involving sophisticated computer-based methodology suitable for the handling of large data sets – von Lampe, 2006) and of course in the terrorism debate. Hence, the

relevance that **Social Network Analysis** (SNA) has achieved in the scientific debate, but also in the law enforcement and intelligence community. Social Network Analysis (SNA) is useful in analysing cases for identifying kinship patterns, community structure and interlocking directorships because it investigates the way they work through networks. SNA can also graphically map out theories (Scott, 1988). Furthermore, SNA is often used in order to perform activities that concern criminal intelligence (Sparrow, 1991). Krebs's model of the 9/11 has been influential (2002). The advantage of this is that it offers insights about the internal structure of the group being analysed. Although SNA faces the problems of (a) incompleteness (the inevitability of missing nodes and links that the investigators will not uncover; (b) fuzzy boundaries (the difficulty in deciding who to include and who not to include) and (c) dynamic (networks are not static, they are always changing), further SNA research has enriched to introduce dynamic network analysis and nonlinear dynamical systems, intelligent adversarial approach and others. This allows SNA to predict and measure the relational ties, their quality and their strength and, consequently, offer useful insights, sometimes counter-intuitive, to disrupt their functioning (Fellman, 2016).



Source: Fellman (2016)

Figure 4. Krebs's original 9/11 network model



Source: Fellman (2016)

Figure 5. Krebs's extended 9/11 network model with centrality

It should be noted that kinship, violence and trust were once considered as external variables that kept the organisation together, however, the networked perspective sees them as interrelated (Von Lampe/Johansen, 2004; Campana/Varese, 2013; Campana 2016). Members and cells of organised crime groups and also terrorist networks have few ties that connect them together, rather each member becomes involved because of the affiliation via a close network friends and family. If, as discussed above, criminal organisations are networks (Varese, 2010b), despite contrary opinions (Powell, 2000), criminal and terror organisations will have a less formal structure than more traditional structures, or they might be an entirely different form of organisation (Williams, 2001). In the case of organised crime groups, especially Mafia, it is not possible to have cells that could continue to exist without the support of hierarchic superiors. From a law enforcement perspective this is why highly connected members and bosses should be tracked down first and an understanding of how organised crime groups and terrorist networks manage to infiltrate a market, pervade territories and shape their interior architecture is essential for practitioners. All of the features

outlined above have specific patterns, methods and motivations and their specific identification as a site of intervention is crucial for an effective disruption of their activities.

Radicalisation, as said, is a core object of literature analysis from many disciplines (social movement and social network theories, psychological, social-psychology and others) with obvious emphasis in Islamist radicalisation. Indeed, despite some similarities, criminological research tends to understand that radicalisation is not really applicable to OC (Decker/Pyrooz, 2011). Others find that better understanding radicalisation might be useful in understanding also the pathway into crime (Wall, 2017). There are many different academic, legal and policy definitions of radicalisation; the common ground being that 'is a process which involves different multidimensional factors and dynamics' (Dzhekova et al., 2016:12). Both root causes and pathways models describe with a different approach this 'multidimensionality' and, therefore they offer insights for TAKEDOWN project's purposes. Root causes models, as said, usually differentiate several levels: a subjacent ground, where external (pull) and internal (push) factors interplay, leading to radicalisation when a triggering event arises. Pathway and stage models opt for looking radicalisation as a progressive process over a period of time where different factors or dynamics occur (Neumann, 2013).

Individuals who are moved by personal victimisation or political grievance seek out and join groups that support their feelings. The process of radicalisation is gradual and also involves high degrees of self-persuasion often assisted by the fact that friends or family members in their network might already be radicalised or indoctrinated. In both organised crime groups and terror networks, specific rules such as the fulfilment of initiation tasks might be applied for an individual to be accepted. Such groups tend to have a higher level of cohesion which isolates them from the rest of society and competes against other groups for support or to exclude less radicalised members. At a mass level, radicalised groups become represented as symbols which themselves function to create fears and reinforce values and direct hate towards a specific set of people. The model of McCauley and Moskalenko (2008) represents this pathway (Table 3).

Level of radicalization	Mechanism
Individual	1. Personal victimization
	2. Political grievance
	3. Joining a radical group—the slippery slope
	4. Joining a radical group—the power of love
Group	5. Extremity shift in like-minded groups
	6. Extreme cohesion under isolation and threat
	7. Competition for the same base of support
	8. Competition with state power—condensation
	9. Within-group competition—fissioning
Mass	10. Jujitsu politics
	11. Hate
	12. Martyrdom

Table 3. The pathway to violence. Source: McCauley/Moskalenko (2008)

Other models of understanding the pathway to serious crime is through the individual's mind-set, such as Borum's four stages (2011[2003])[20] or Moghaddam's narrowing staircase to terrorism (2005). These processes are said to involve individuals who believe they have no voice in society, and in cases of suicidal terrorism to be encouraged by a '**significance quest**' accompanied by various

[20] This model – developed as a training heuristic for law enforcers - uses a four-stage process that 'begins by framing some unsatisfying event, condition, or grievance (It's not right) as being unjust (It's not fair). The injustice is blamed on a target policy, person, or nation (It's your fault). The responsible party is then vilified—often demonized—(You're Evil), which facilitates justification or impetus for aggression' (Borum, 2011:39).

ideological reasons (Kruglanski et al, 2009). Both suicidal and despaired seem to respond to the **frustration thesis** (McDonald, 2013), which combines the feeling of 'weakness, irrelevance, marginalization and subordination experienced by Muslim people' with the memory of a glorious past of a great transnational civilization (Toscano, 2016:123).

Sinai's model of radicalisation (2016) aggregates components of both root causes and pathways models in order to explain jihadist violent extremism and foreign fighters in Syria and Iraq and identify critical points for preventative intervention (Figure 7, in following page). The pathway to violent extremism is started by individuals or groups who are indoctrinated and incentivised to adopt increasingly intolerant and extremist political and/or religious beliefs and behaviours, ranging from aggressive proselytizing to violent extremism. Two of those factors, a personal crisis and domestic issues, **push** the individual to join an organisation which listens to them or represents their views. Individuals embrace extremist ideologies after feeling socially marginal and downgraded by others, often accompanied by family, relational and/or employment problems and a sense of uprootedness and alienation from their own or the host society. They are also driven by personal or group-specific grievances such as beliefs that society is discriminating against them and co-religionists rather than accepting them as equals.

There is also another range of factors that **pull** the individual into joining an extremist group, these include foreign issues, sub-cultures, local radicalisers and social media influence. People might, for example, feel outrage at the unjust suffering of co-religionists in a foreign conflict to which a Western government, in their view, is indifferent or hostile. Sometimes extremist ideologies spread by local radicalisers and recruiters are pervasive and attractive, whether they might be preachers, community leaders, jihadist veterans, or other operators and facilitators, working by means of family and friendship networks. Extremist groups also employ social media tactics including websites, online magazines, or Twitter and YouTube videos. The latter featuring influential spiritual and jihadist leaders promoting extremist activities on behalf of their cause, including becoming fighters on behalf of their co-religionists in a foreign conflict. Vulnerable individuals 'buy' into and accept these polarizing narratives and reject Western values while embracing jihadist interpretations of Islam, Anti-Christian, anti-Semitic and anti-Shia hate rhetoric. The attraction for this kind of world drives them to act, but the actual **triggers** of action might include, a personal crisis or media-transmitted narratives of suffering of co-religionists. They might develop, for example, the belief that there is a need to join insurgent groups to avenge for the death of their associates, even if these are neither family members nor friends, and that it is their religious duty to embark on warfare to defeat the enemies of their religion.

This process might ultimately lead the individual to prepare for **travel** to a foreign conflict zone. This is done first by intensifying contacts, say, with 'returnees', recruiters or facilitators that will enable them to enter the conflict zone; start to make travel plans; adopt a 'cover story'; and start selling/ giving away personal possessions. The travel must, however, be funded. This might be done by depleting a personal bank account, seeking donations from associates or others for the foreign travel, receiving funds from unexplainable sources such as radicalizers/ recruiters/ jihadi charities who manage such travel, or by engaging in illicit or (organised) criminal activities such as credit card fraud. Logistical facilitators might be sought within their local community or via the Internet in order to enable foreign travel. Eventually, transit routes are chosen via bordering countries, such as Turkey, which may or may not require entry visas. When in-country, local smuggling facilitators collect Western recruits at airports and transport them to safe houses at designated border towns for eventual smuggling them into Syria or Iraq. Once at their conflict zone destinations, individuals are

likely to become fighters, or martyrs or receive training and indoctrination for deployment upon their return to their Western countries of origin. A minority of these might return to their (often Western) home countries for reasons ranging from disillusionment with fighting in harsh battle environments, or to become radicalizers, recruiters, sleepers, or terrorist operatives in their home countries.

Pathways into Jihadist Violent Extremism In-Country & Becoming Fighters in Foreign Conflict Zones	***Description***	***Preventative Measures***
Category I: **Radicalization Factors**	A **process** by which individuals or groups are **indoctrinated** and **mobilized to adopt increasingly intolerant and extremist political and/or religious beliefs and behaviors**, ranging from aggressive proselytizing to violent extremist.	**Preventative Measures**: **"Soft" multidisciplinary programs** to counter extremist ideologies, promotion of social cohesion and socio-economic integration in society, law enforcement programs to identify and apprehend extremist radicalizers.
I-1 - Push Factors: Personal Crisis	**Cognitive opening** ("born again"-type) to embrace **extremist ideologies** due to **feeling socially marginal** and downgraded by others, often accompanied by family, relational and/or employment problems, and a **sense of uprootedness and alienation** from own or host society.	**Preventative Measures**: Focusing on **integration into society and economy** by addressing discrimination and other issues that give rise to personal grievances. Target at-risk individuals to **make them more resilient to extremist ideologies**; implement individual self-empowerment programs.
I-2 - Push Factors: Domestic Issues	Personal and/or group-specific grievances such as beliefs that host or own **society is discriminating against them** and co-religionists **rather than accepting them as equals**.	**Preventative Measures**: Promoting a **sense of belonging and shared identity through interpersonal dialogue at grassroots level**, anti-discrimination projects, improving educational opportunities, and encouraging non-violent and legal ways to address grievances.
I-3 - Pull Factors: Foreign Issues	**Feeling outrage** at the **unjust suffering of co-religionists in a foreign conflict** to which one's Western government, in their view, is indifferent or hostile.	**Preventative Measures**: **Counter-narratives that Western government involvement in Syria (and Iraq) is not motivated by religious Christian antipathy towards Islam**.
I-4 - Extremist Sub-cultures/Local Radicalizers	**Pervasiveness of extremist ideologies** that are spread by local radicalizers and recruiters, whether preachers, community leaders, jihadist veterans, and other operators and facilitators, working often by means of family and friendship networks.	**Preventative Measures**: Outreach programs that cooperate with responsible local community leaders to counter extremist ideologies with **counter-narratives and self-empowering programs** that promote constructive engagement in society rather than a turn to violent extremism.
I-5 - Social Media & Influential jihadist or religious Leaders	Extremist groups employ **social media venues**, incl. websites, online magazines, or Twitter and YouTube videos, featuring **influential spiritual and jihadist leaders** to promote extremist activities on behalf of their cause, including becoming fighters on behalf of their co-religionists in a foreign conflict. Vulnerable individuals "buy" their polarizing narratives and reject Western values while embracing jihadist interpretation of Islam. Anti-Christian, anti-Semitic and anti-Shia hate rhetoric	**Preventative Measures**: **Vetting and monitoring extremist social media websites**, countering their extremist leaders with **counter-narratives to encourage disengagement from extremism** and discouraging travel to foreign conflict region.
Category II: Triggers	Triggers might include, a personal crisis or media-transmitted narratives of suffering of co-religionists; a **belief that there is a need to join insurgent groups to avenge for the death of their associates** (even if these are neither family members nor friends) and that it is their religious duty to embark on warfare to defeat the enemies of their religion.	**Preventative Measures**: To counter such triggers, **utilizing disillusioned returnees** or local community leaders **to dissuade potential recruits** from traveling through messages such as explaining that they will be exploited as 'cannon fodder', that the insurgents themselves are committing brutal atrocities against innocent fellow Muslims, and that their potential travel or resort to terrorism will serve to destroy any chances for advancement in their own societies.
Category III: Preparation for Travel to Foreign Conflict Zone	Prepare to travel to the foreign conflict zone by taking measures such as **intensifying contacts with 'returnees'/recruiters/facilitators** that will enable them to enter the conflict zone; **start to make travel plans**; **adopt a 'cover story' for their travel**; and **start selling/giving away personal possessions** because they realize they may never return.	**Preventative Measures**: **Identifying the warning signs** that an individual may be preparing to embark on suspicious travel to a foreign conflict zone and **dissuading or preventing** such travel by taking away passports.
III-1 - Funding Sources	Fund travel by **depleting one's personal bank account**, **seeking donations** from associates or others for the foreign travel, **receive funds from unexplained sources** (e.g., radicalizers/recruiters/jihadi charities who manage such travel), or engage in **illicit activities such as credit card fraud to raise funds**.	**Preventative Measures**: **Monitoring and tracking suspicious funding activities** to facilitate travel to a foreign conflict zone.
III-2 - Logistical Facilitators	**Seeking logistical facilitators in a local community or on the Internet** to enable foreign travel.	**Preventative Measures**: Monitoring and tracking those who contact logistical facilitators.

III-3 - Transit Routes	Transit routes stretch from **countries of origin to bordering countries**, such as Turkey, which may or may not require entry visas. Once in-country, **local smuggling facilitators** collect Western recruits at airports and transport them to safe houses at designated border towns for eventual smuggling them into Syria or Iraq.	**Preventative Measures**: **Multilateral and bilateral level monitoring programs** that collect data on suspicious foreign travel and the logistical networks that smuggle them to their destinations.
Category IV: Activities in Syria or Iraq (Fighting, Training or, less often, Humanitarian Aid)	Once at their conflict zone destinations, Westerners are likely to **become fighters**, or martyrs or **receive training and indoctrination** for deployment upon their return to their Western countries of origin.	**Preventative Measures**: **Monitoring and tracking these individuals' movements and activities**, such as in social media, including contact with their families and associates in their home countries.
Category V: Returning to Western Countries of Origin	**A minority might return** to their Western home countries, for reasons ranging from **disillusionment with fighting in harsh battle environments**, to even further radicalization upon **completion of their training and indoctrination** to become radicalizers, recruiters, sleepers or terrorist operatives in their home countries.	**Preventative Measures**: **Canceling passports, revoking residence permits and denying re-entrance** to home country's border crossings, arresting returnees at border crossings, or **permitting them to return but tracking their activities** in their local communities, or engaging them in programs to de-radicalize and disengage them from terrorism.

Table 4. Framework for modeling the radicalisation and mobilisation pathways into jihadist terrorism and intervention points for effective preventative countermeasures. Source: Sinai (2016)

Closely connected to radicalisation lies **recruitment** which has been understood as a way of bringing a radical into the circle of organised terrorist activities, but it is not easy to determine whether those who join a TN act or are acted upon (McDonald, 2013). However, individuals eager to join terrorist networks – **foreign fighters -** pose serious security risks to insurgent entities. Hence the necessity to filter the recruitment process through mediators or facilitators. These not only make the process more opaque to law enforcement but also guarantee a selection of sort of the would-be recruits. Those who are recruited, however, may not always be total novices or amateurs, as their identity and political inclination may already be well known to law enforcers. Recruitment, in the spreading 'network of cells', may take place in the guise of **self-affiliation**, with individuals or small groups mimicking the acts that they presume are consistent with the strategy and practice of the organization they would wish to join. The terrorist organization, in this way, can rely both on its own operative members and on a range of sympathizers scattered around the word. The latter, even when devoid of any practical connection with the 'mother' organization, in effect carry out its policy. Isis, for instance, owes its strength not only to its specific military power, but also to the exemplary nature of its acts that may be replicated by '**lone actors**', who feel legitimized to kill after internalizing the deadly philosophy of the organization.

A third aspect, namely the geographical dimension, must be addressed. '**Territoriality'** plays indeed a very important role in understanding OC/TN, particularly nowadays when the emphasis in transnationalised OC and global terrorism is deemed as compelling. Europol and national LEAs take cooperation between OC groups servicing black markets as an established fact. Conceptualisations of OC as illegal entrepreneurs thus turn territoriality into markets and try to find in economics some explanations of how they work internally (entry conditions and market functioning) and externally (transnationalised). It also explains why ICT can have an impact on offline (criminal) markets and the difference market conditions that may prevail in the cyberspace.

The reasons why OC appears in a concrete territory (market) could be the explained because of the existence of a 'demand for Mafia'. Gambetta and Reuter (1995) resume those '**entry conditions'** (Table 6 below text): low product differentiation, absence or low barriers to entry (McAfee/Mialon/Williams, 2004) – which can also be the previous presence of a criminal organisation, a reputational barrier only leaving collusion as non-violent way of entry -, low technological innovation level, unskilled labour force (Varese, 2011), inelastic demand – which is likely in illegal products, but can also obtain in legal markets (Albanese, 2008); high number of small

size firms – which impedes resisting collusion, although big companies may also profit from collusion with OC to assure a captive market (Saviano, 2006) -, and existing labour unions – liable to be corrupted (Block/Chambliss, 1981). The size of a territory influences Mafia's ability to penetrate its markets: the smaller, the easier. It should be noticed that the market just described is hardly to be export-oriented, so the firms compete in the same territory and the need of a ruler or protector may emerge. Once a Mafia breaks into a market it offers 'efficient and convenient' services in order to patronize the largest stake of firms, however, Mafia clans seek to monopolise protection in a specific neighbourhood or market and they subsequently dictate different or deferred payment solutions according to the size of the firm. Some authors have analysed cases that seem to replicate this picture (Varese, 2011; Lavezzi, 2008). However, Gambetta and Reuter argue that Mafia cannot rise and settle if there is no demand for a specific illicit service. Such a service can be only supplied by OC because the State cannot offer it for legal or for public order reasons. Yet, the activity Gambetta and Reuter analyse is one of those that create a 'demand for Mafia', and such demand is prodromal (manifested in different ways) in a market where organised crime wants to offer its services (Lavezzi, 2014; Varese, 2006). Finally, it should be noticed that the existence of cartels (agreements amongst producers of goods or services in a specific market which aims to limit, restrict and rule competition in order to get higher profits than would be obtained in a free market status) might create the same need for a third party, acting as a ruler.

ENTRY CONDITIONS	FEATURES
Product differentiation	Low
Barriers to entry	Low or not existent
Technology	Low
Labour skills	Unskilled
Demand for products	Inelastic
Number of firms in the market	High
Size of the firms in the market	Small
Labour unions	Present

Table 5. Entry conditions ('Mafia Demand'). Source: Adapted from Gambetta/Reuter (1995)

As to **cooperation between criminal organisations**, the entrepreneurial strand has found replicas of the cooperative business relationships in the criminal stage. Williams follows this line showing that the benefits of cooperation outweigh its costs and risks and that OC groups in fact display a number of business-like cooperative endeavours (from barter to supply, to tactical to strategic alliances), although, for him, territoriality still gets in the picture through the notion of 'spheres of influence' (Williams, 2002). Those possibilities are displayed in Table 6.

Type of Relationship	Forms of Cooperation	Characteristics of Cooperation	Benefits of Cooperation
Strategic alliance	Operating linkages Franchise Licensing	Long-term High level of trust	Co-opt potential adversary Synergies facilitate market entry Complementary expertise Exploit global-local nexus
Tactical alliance	Operating linkages Licensing	Short-term Developing moderate level of trust	Synergies facilitate market entry
Contract and service	Related to specialized tasks	Employer-type relationship	Use specialized skills
Exchange	Barter arrangements	Short- or long-term Limited to product exchange	Extend product range and develop new markets
Regular supplier	Supplier-customer	Degree of trust and predictability	Highly efficient and adaptable
Short-term supplier	Wholesale to retail	Expedient and instrumental	Provide interim solutions to meet market demand

Table 6. Cooperative relationships in the business world. Source: Williams (2002:69)

This 'natural' cooperative drift also occurs across boundaries making appear the notion of '**transnationalised organised crime'** (TOC) that, due to state jurisdictions, inevitably must be addressed by means of international cooperation (UNODC, 2012b). Hence the central position that TOC has achieved in international and regional fora (notably United Nations, the G8, OECD, Council of Europe, OAS and others) and within states' foreign policies; the EU being in this aspect a leading international, not entirely normative though, actor (Ruiz Díaz, 2015). While it is important to warn against the idea that OC stems from abroad (some sort of a foreign foe menacing our security), it is undisputable that the social, economic and political changes that are usually assigned to 'globalisation' have facilitated and still do the conditions for TOC to flourish and prosper. In von Lampe's review of TOC literature all the abovementioned cooperative relationships occur (2013). This trend, whose epitome could be found in the cyberspace, has led some among which LEAs and international institutions stand out to describe a picture of criminal networks and organisations with a transnational or multi-ethnic composition that have reached global impact (Sansó Rubert (2016), who even explores the utility of geopolitics in understanding the international strategies of most serious OC – i.e., those disputing states the territorial control and use of violence). Notwithstanding, the transnationalisation of OC and TOC require some **qualifications when facing national contexts**, showing '*fluid, multiple dynamics* guiding the ways in which groups create *associations* and *affiliations*' (Ruggiero, 2016:16)[21]. In fact, as Varese (2001 and 2011) has pointed out, criminal organizations are mainly stationary, because it is at the local level that they provide their services and goods while accessing resources. Looking at the European OC landscape, von Lampe also insists upon the need to be cautious on this global market allegory. Neither OC can be reduced to the

[21] Ruggiero affirms: 'In the Netherlands, for example, the situation is characterized by the co-presence of distinct groups, which may cooperate, but only on the basis of a precise division of roles. Such groups, in fact, are unlikely to form organic, long-term partnerships, let alone establish collegial, intra-ethnic memberships. Ethnicity is also a key variable in Greece, although ad hoc partnerships may be influential in some criminal activities. In France and Italy, on the other hand, indigenous criminal groups may act as gate-keepers, allowing access to illicit markets to non-nationals only at pre-established financial costs. In both countries, however, newcomers may also operate in illicit market sectors dismissed by upwardly-mobile local groups. In Italy, moreover, rather than partners, the newcomers may well provide 'criminal labour' to locally established criminal networks. Mixed ethnic groups may be taking shape in Spain, but are extremely rare in Russia, while in the UK what is vividly manifest is a situation of competition and succession among ethnicities, rather than their amalgamation' (ibid:16)

provision of illegal goods or services, nor are illegal markets, such as the drug market, impervious to national, even regional idiosyncrasies, which means that 'illegal markets cannot be created at will. Supply does not automatically meet demand and vice versa. Rather, illegal markets are the product of a fairly complex interplay of diverse factors' (Von Lampe, 2008). Furthermore, evidence of the involvement in transnational crime by established noneconomic criminal organizations (the Italian mafia-type organisations, the Russian and Georgian *vory v zakone* or a Chinese triad) face to illegal enterprises is too limited so as to endorse a trend towards a globalization of control of criminal activities exerted by established criminal organizations. The picture that emerges from empirical research is more complex, often more mundane, though not necessarily less serious, than popular imagery of global mafias (Von Lampe, 2013).

Finally, before moving onto the issues of OC/TN nexus and the centrality of the cyber dimension, some remarks in relation to **countering measures** should be made, even though many considerations have already been raised along the previous sections. This baseline report cannot possibly offer an exhaustive list of those social, technical, legal and policy measures put in place, let alone followed by the critical assessments that scientific literature has devoted to many them. Some are presented in the following:

- The EU and MS response has excessively focused on TN face to OC with the correlative shifting of public funds and resources. This has been said to create and nurture a state of public anxiety or 'moral panic' that feedbacks TN, particularly when military action is taken, by overestimating their power and credibility as a threat (English, 2016; Mueller/Stewart, 2016; Ramadan/Shantz, 2016) and producing preventative counter-productive effects nourishing fear and encouraging suspicion and racism (Mythen/Walkate, 2006; Ahmed, 2015, Abbas/Awan, 2015) as well as 'backlash effects that led to greater numbers of crimes' (Chermak/Freilich/Caspi, 2010:139). It has also reduced the scope of human and financial public resources aimed at fighting OC, resulting in an enforcement selective action, as certain groups have been prioritized while emergent ones have been partly neglected (Jacobs/Wyman, 2015). With law enforcement resources increasingly shifting towards terrorism, institutional action against organized crime is now limited to routine intervention based on electronic surveillance, informants and undercover policing. Witness Security Programmes have been in place for decades, when the code of *omertà* began to break down and turncoats were rewarded with lenient sentences. Prosecutions for tax offenses and asset confiscation have also been widely used (ibid.). This statement regarding USA seems applicable to EU and its MS and while focused on 'crime in association', it does not look tailored to effectively taking down 'crime in organisation' (Ruggiero, 2016).

- The institutional framework is extremely complex and liable to suffering from functional duplicities, waste of public resources in times of austerity or even contradictory strategies and/or measures. The policy-cycle determined by threat assessments has been considered questionable and liable to encompass or convey narrow partial priority perceptions that overestimate those threats and their social impact as well as determining ineffective enforcing policies (Edwards, 2016; Bianchi, 2017).

- As regards to legal measures, the direction to enlarge criminalization by incriminating preparatory stages as well as to export that approach towards third states have merited criticisms by legal doctrine and authors that point up its impact on the integrity of other European policies (such as migration or asylum) and damaging the reputation of the EU as an international normative actor (Ruiz Díaz, 2015). This pre-crime strategies, especially regarding terrorism, are

said to centre state action on sheer suspicion, whereby individuals and groups are targeted without a specific charge being formulated. Anticipating risk, in this sense, tends to integrate national security into criminal justice, to the detriment of civil and political rights (McCulloch/Pickering, 2009). Despite the 'heavy legal package' that the EU has prompted dealing with money-laundering, confiscation of assets and so on, there still remains critical differences in national legislation (or in the 'common legal measures' implementation) that hamper international cooperation and effective prosecution (Yordanova/Markov, 2012).

- The emphasis on mass surveillance mechanisms with undifferentiated extensive collection of personal data is another matter of great concern as different national and international courts have confirmed on several occasions. Some landmark decisions of the ECJ have been recalled earlier, but this is also the case of the ECtHR whose recent judgment in *Aycaguer v. France* (Appl. 8806/12) concerning DNA collection for a menial offence just piles up. Here, useless duplicities and operational deficiencies have been mentioned (Bianchi, 2017).

The feature that is important to stress for TAKEDOWN Project relates more to the responsive approach that has been established at the EU and MS levels, because of its repercussions on the model design that TAKEDOWN intends to elaborate. This approach has come to surface once and again along this baseline report as to the need of holistic, multi-faceted strategies, policies, measures and tools that require involving different public and private stakeholders and may call upon many different public services[22]. This notion can be illustrated by the European Counter-Terrorism Strategy mentioned earlier that signals four different strands in the well-known PPDR: Prevent, Protect, Disrupt and Respond (Figure 6, next page).

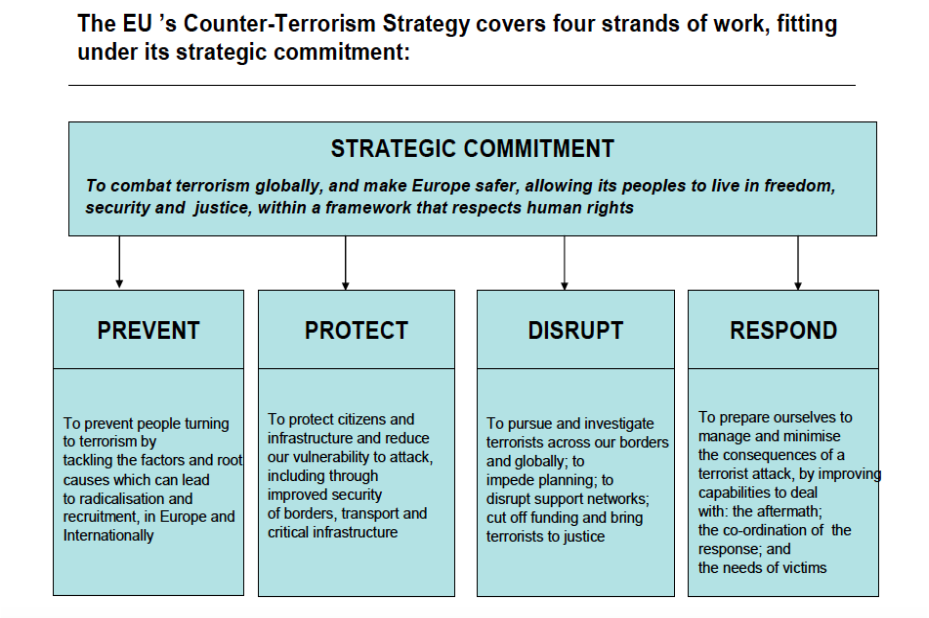


Figure 6. EU counter terrorism strategy. Source: EU (2011)

The boundaries between those four strands are arguably porous, in particular because the prevention category is a contentious field with a certain conceptual attraction power (*vis attractiva*)

[22] TAKEDOWN Deliverable 2.5 has collected a number of public security services (PPS) retrieved from MS, such as helplines, reporting platforms, information hubs, and contact points, which are supporting the public in case of risk. This deliverable defines more precisely what conditions should be met to qualify as a PPS. The screening as to May 2017 included 97. Most of them only have a national scope and consist of reporting platforms or information hubs mainly dealing with radicalisation, cyber-crime and cyber-terrorism, emergency and crisis communication (Bonfanti, 2017).

and sometimes is defined by the non-intervention of law enforcement services whereby it might be hard to say to what extent a certain measure should be considered preventative or pro-active policing (disrupting). However, they clearly show anyway that in order to treat OC/TN many avenues are open and pertinent because they would point to future possible actors (discouraging engage into OC/TN), future victims (enhancing against OC/TN), current actors (weakening or neutralising OC/TN) and current victims (limiting damage caused by OC/TN). Having regard to the multi-dimensional nature of these phenomena, OC and TN cannot possibly be reduced to law enforcement (eventually accrued with military action) but demand instead this much broader approach that involves different actors and non law-enforcement agencies. There is no doubt that preventing, when addressing the root causes of OC/TN, needs to mobilise all those other public agencies and private stakeholders that can foster social cohesion and equality. Educational programs, economic investment in deprived areas and vulnerable groups, enhancing public services and governance, fostering inter-community dialogue and reducing discrimination undoubtedly address the structural conditions where OC/TN flourish and feed. Reducing social vulnerabilities calls for improving regulation so as to fill the legal, technical or other gaps that are exploited by OC/TN, to which the private sector can also contribute and sometimes be even more effective than just policing (Levi/Maguire, 2011). Minimising the harm caused by OC/TN requires not only a swift response on account of public authorities that includes law enforcement and other public agencies, but it relates as well with society at large. The prison system and de-radicalisation are self-explanatory examples. Thus this non-traditional perspective suggests a more holistic and multi-agency approach (Levi/Maguire, 2004; Wall, 2015; Sinai, 2016) where not only the public sector, but also community, policy makers and the private sector have a say. Table 7 below summarises this non-traditional approach that is today the common currency at least on a strategic level. However, this multi-agency intertwining, it has to be said, also creates some grey areas, notably when they amount to the involvement of community, private stakeholders and non law-enforcing public agencies in anticipatory pursuing and prosecuting OC/TN (Bianchi, 2017).

Community approaches	1. Community crime prevention 2. Passive citizen participation: giving information about harms and risks, hotlines 3. Active citizen participation: civic action groups
Regulatory, disruption and non-justice system approaches	4. Regulatory policies, programmes and agencies (domestic and foreign, including non-governmental organisations and IGOs such as the IMF, OECD/FATF and World Bank) 5. Routine and suspicious activity reporting by financial institutions and other bodies 6. Tax policy and programmes 7. Civil injunctions and other sanctions 8. Military interventions 9. Security and secret intelligence services 10. Foreign policy and aid programmes (US 'certification' of countries as adequate/inadequate in their anti-drugs measures)
Private sector involvement	11. Individual companies 12. Professional and industry associations 13. Special private sector committees 14. Anti-fraud and money laundering software 15. Private policing and forensic accounting

Table 7. Non-traditional approaches. Source: Levi/Maguire (2011)

In this regard, it should be recalled that this response mostly falls within the MS competences, since it is related to fundamental social and political choices incumbent upon them. So national practices, policies and measures differ greatly as de-radicalisation might again illustrate. Consequently, for

TAKEDOWN's modelling purposes (Figure 8, in next page), all kinds of interplay between the different stakeholders involved has to be conceivable, the purpose being to get a comprehensive picture of those varied interactions, enhancing inter-stakeholders communication and experience exchanging so as to identify best practices, functional or operational obstacles and needs, improve efficiency reinforcing synergies between them and assess their potential transferability to other MS. In other to proceed with the empirical research and ulterior validation, TAKEDOWN Project has already collected a fairly significant number of stakeholders (976 as of 30 April 2017) coming from more than fifty countries. Those stakeholders have been aggregated by target groups in eight different categories as shows the following Figure.

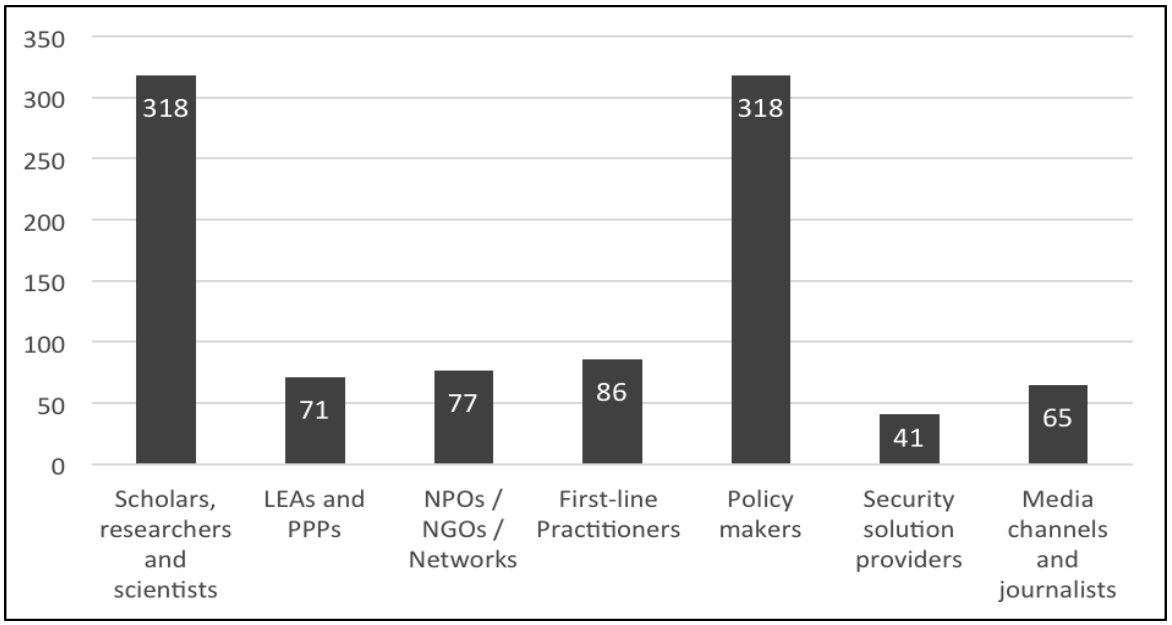


Figure 7. Collection of stakeholders: Distribution of stakeholders per target groups. Source: Markov/Ilcheva/Yordanova (2017) TAKEDOWN Deliverable 2.3

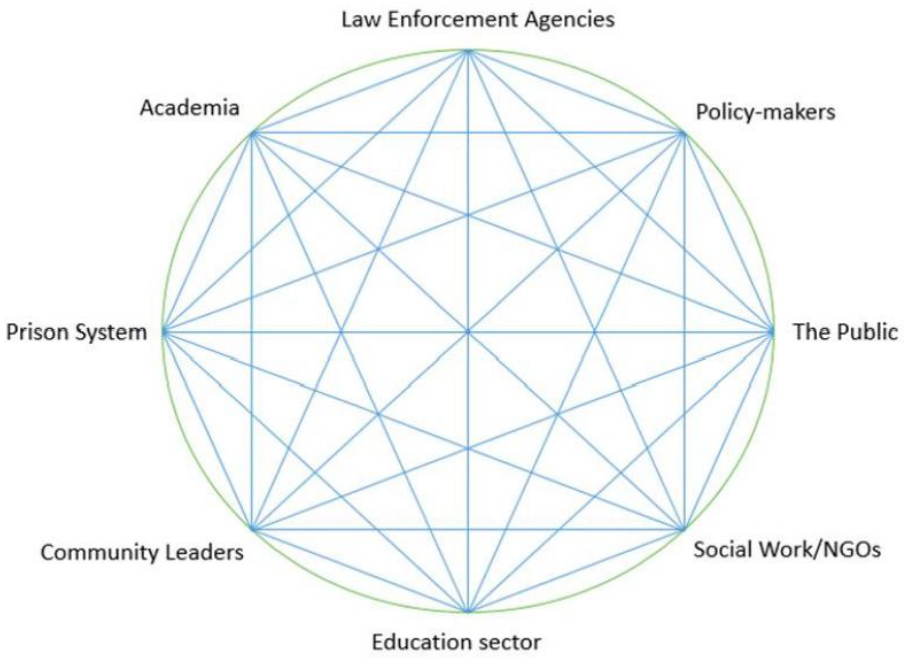


Figure 8. Stakeholders interactions. Source: PATRIR (Partner of TAKEDOWN Consortium)

3.3. From Separate Clusters to Impure Hybridization: the Nexus between Organised Crime and Terrorist Networks

Traditionally OC and TN have been seen as separate clusters that coexist. In this model, OC/TN groups share the same geographical region where they concurrently pursue different aims through different activities and by different methods, whence they should be approached by law enforcement in a compartmentalised way. Whereas OC is profit-driven, TN has a distinct political aim so their overlaps would seem to respond more to a **cross-instrumental rationale** (i.e. *epiphenomenal*), mainly profit coming from only certain ('ethical') types of criminal activities as an additional tool for funding the terrorist group and violence as a supplementary and infrequently used tool of OC groups for negotiating their presence in illegal markets. Their strategies towards public attention and/or their places within the illegal-legal continuum, not to mention their respective self-depictions, would also definitely detach both phenomena.

However, over the last decade the issue of the nexus between OC and TN has received increasing attention by policy-makers, LEAs and academia, yet with inconclusive results. At the international level, the nexus emphasized has been international terrorism **financing** through transnationalised OC – UNSC Resolution 2195 (2014), although the Secretary-General Report based on this resolution admitted that 'both are distinct phenomena, and have different modus operandi, aims and international legal frameworks (S/2015/366, 21 May 2015). As far as LEAs, the Europol SOCTA emphatically mentions this nexus without offering a deep clarification about the nature of those links (Europol, 2017a), which might be explained precisely because the prosecution and law enforcement perspective that they take blurs or naturally neglects the difference between both OC/TN (Zöller, 2012). Academia on its part has developed a rich debate that it is still contentious. As the EU project CT-Morse describes: 'Whether referred to as a 'nexus', or framed in terms of related issues of convergence, transformation and hybridity, one thing remains clear — there is no consensus, and a tendency for scholars to talk past one another, even when in agreement about some of the most important factors being analyzed' (Reitano/Clarke/Adal, 2017). Thus some scholars reject the assimilation of both phenomena as politically intentional (Ruggiero, 2010b) or because a hasty unification may lead to potentially ineffective preventative and enforcement measures (Levi, 2014; Sergi, 2016) due to the still fundamentally different nature of the aims they pursue (Campbell, 2014; von Lampe, 2016). Some other authors deny that the difference in aims is actually as clear-cut as it is presented by this 'methods, not motives' framework (de Boer/Bosetti, 2015) and that there is a 'terror-crime' continuum on which groups can oscillate and occupy several intermediate stages (Makarenko, 2004). Others claim that both phenomena are ultimately incompatible over the long term (Picarelli/Shelley, 2002; Naylor, 2002).

Different academic approaches have offered different classifications depending on their respective point of view, but they may be referred to three different categories: confluence, cooperation and transformation. Some factors seem to have made this nexus look different or at least thicker, such as the diminution in terrorism 'legal funding' (sponsoring states and private donors) and the effects of financial CT regulations, the change in TN structure and methods acting in a more decentralised manner, including small cells and low-cost attacks as well as the modification in armed conflict dynamics, especially in fragile and failed States (Marrero Rocha, 2017).

The **confluence** realm has been extensively explained with regard to the TN use of classic OC activities for **fundraising** and to the less frequent use of terror methods by OC groups to make a political stance against a more committed prosecuting public policy. The move towards criminality of

terrorist groups that have abandoned political struggle or lost social support is also known. However, there may be new developments that deserved rethinking. This OC-profit source of TN has gained crucial importance because of the reduced costs that current decentralized terrorist cells and lone actors need to pursue an attack, ranking as its current second funding source (Oftedal, 2015). The frequent criminal record of these 'new' terrorists has also been identified as significant as well as it is the attention paid to criminal past in TN recruitment processes (Reitano/Clarke/Adal, 2017). However, whether this is a new type of actors' transformation or these criminal backgrounds make more sense within the more general understanding of the radicalisation process is still to be determined and further research seems compulsory (Basra/Neumann/Brunner, 2016). On the other side of the spectrum, some **terrorist organizations** such as Hezbollah or IS seem to have passed an instrumental level and have actually engaged in OC structures and international criminal markets with a more determined approach and strategy[23]. Other terrorist organizations such as Al-Qaida in the Islamic Magreb, Abu-Sayyan or Al-Nusra seem to rely heavily on criminal activities for funding.

The establishment of **cooperative relationships** between OC and TN because of **logistic** and/or **operational** needs (such as profiting of criminal routes or safely crossing the territory controlled by a terrorist group) or through the exchange of illicit goods or services (arms, drugs, money, explosives or training) has also been well documented (Grabosky/Stohl, 2010). The more problematic nexus particularly appears when within the setting of a protracted conflict, where no public authority whatsoever is deployed, the respective agendas of OC and TN blur and enmesh with each other's to the point of giving birth to a **proper hybridization**, as the current case of Libya and Trans-Sahara may show (Marrero Rocha, 2017). In Figure 8 below, these connections may be observed.

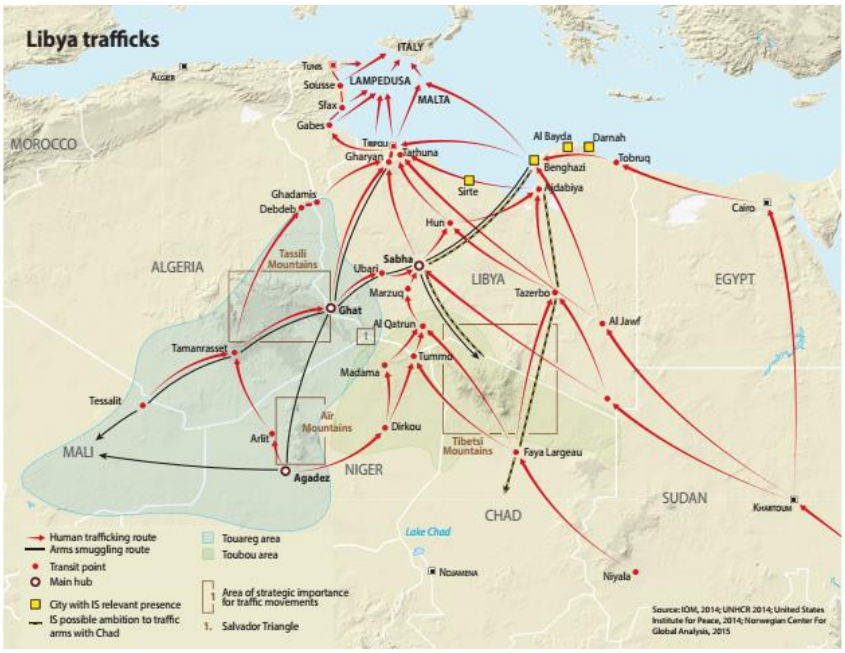


Figure 9. Organized crime – Terrorist networks nexus in Lybia. Source: RHIPTO/Global Initiative Against Transnational Organized Crime (2015)

[23] In February 2016, investigations by U.S. and European law enforcement led to the revelation that Hezbollah's terrorist wing, the External Security Organization (aka the Islamic Jihad Organization), runs a dedicated entity specializing in worldwide drug trafficking and money laundering. The investigation spanned seven countries and led to the arrest of several members of Hezbollah's so-called Business Affairs Component (BAC) on charges of drug trafficking, money laundering, and procuring weapons for use in Syria (Hewitt, 2016). Hezbollah's involvement in illicit traffics in Africa is also well documented (de Andrés, 2008).

3.4. The Importance of the Cyber Dimension

Cybercrime is maybe the field where the scientific literature, including practitioners' contributions, and official accounts have more clearly claimed for the need of further research effort (Carrapico/Lavorgna, 2015). Not only the concept remains extremely elusive, but also the empirical data, especially when it comes to measurement its social and economic impact, seem to offer less reliability in order to realistically assess the level of the threat or deduce policy orientation, not the least because of national law enforcement legal, institutional and statistical discrepancies, underreported rate, etcetera (UNODC, 2013; Yordanova et al., 2014). Not surprisingly it has been said concerning organised cybercrime that 'the already exaggerated notion of OC risks have been exaggerated even further' (Leukfeldt/Lavorgna/Kleemans, 2016). Indeed, OC/TN seem so far not to have reached the most dangerous possibilities that theoretically **cyberspace** offers to them, such as engaging in cyberterrorist attacks to critical infrastructures or becoming the private remit of most hierarchical OC groups (Mafia-style) (Lavorgna, 2015, who mentions illicit gambling as an exception where the Mafia could actually expand its market by getting online). However, this does not prevent new information and communication technologies (ICT) from having deeply affect and **transform crime** (Wall, 2007), and consequently law enforcement counterpart so as to arising new legal and operational obstacles in pursuing and prosecuting cyber offences – mainly due to its **de-territorialised** or global nature - but also as to opening extraordinary new police investigative techniques and evidence-gathering tools. Interconnectivity, datafication of everything, automated malware and so forth are trends in current cyber criminality that are not going to decrease but quite the opposite (Koops, 2016) and for that the cyber dimension cannot be avoided in approaching OC/TN at present.

Certainly, cybercrime and **cyberterrorism** themselves remain concepts that have not achieved any common definition at the academic, policy or legal levels and numerous classifications may be found. Wall suggests distinguishing between *crimes against the machine, crimes using the machine and crimes in the machine* (2015:75), which slightly differs from others focusing on the interrelation between real and cyberspace (Luiijf, 2014) or the more usual international legal approach dividing it into typical cybercrimes and other cyber-dependent crimes. Regarding TN Brenner's classification emphasises that the Internet may be used as *weapons of mass destruction, weapons of mass distraction and weapons of mass disruption* (2006). Without expanding on the obvious consequences of this uncertainty as to the academic, legal and political concept, there is no doubt in affirming the crucial impact that digital and networked technologies have deployed over crime and terrorism. A notorious first impact lies on the enlargement and easing of criminal OC and TN activities (Leukfeldt/Lavorgna/Kleemans, 2016). ICT have of course opened **new criminal markets** that are of a global scale, but have also facilitated or enriched more traditional ones by providing new and more **efficient criminal methods** – e.g. in money laundering - or by hindering police detection of criminals' trace (Lavorgna, 2015). These enlargement and facilitation are also to be increased because of the substantial decrease in computer skills and knowledge needed to commit a cybercrime. Criminal malware has become user-friendlier and the emergence of **CaaS** at disposal in the digital underworld has definitely detached cybercrime from the lonely tech-kiddie stereotype, whilst ironically the need for high tech-skills and tools is ever-growing within the LEAs.

As to TN, the use of internet has been extensively studied and known. Gilmour, following the UK Terrorism Act 2001, divides **cyberterrorism** in three categories: *pure cyber terrorism*, cyber terrorism (or *cyber dependent crime*) and *cyber enabled terrorism* (2015). The UNODC report 'The use of the Internet for terrorist purposes' identifies these purposes: propaganda, financing, training, planning,

execution, cyber-attacks (UNODC, 2012a). Dzhekova et al. (2016), after a more detailed classification – **psychological warfare; publicity and propaganda; data-mining; fundraising; networking and information sharing; planning and coordination** -, thoroughly analysed the issue most debated in literature, which is radicalisation and recruitment. The impact of internet and networks in the radicalisation process is not to neglect, particularly in expanding propaganda and reaching wider audiences, reinforcing extremist rhetoric justifications and legitimacy or providing meaningful eco-chambers, but empirical research show that *pure virtual radicalisation is rare* – let alone self-radicalisation - and particularly *recruitment does not occur nor can be completed outside the real world* (ibid.)

Related to these processes, a second relevant impact of internet resolves around the criminal **pathways into cybercrime** and particularly from technology talented curious youth, to cyber juvenile delinquent, to lone cybercriminal to organised cybercrime (Aiken, 2016). In understanding this pathway, 'whereas theories of criminology may explain deviance and anti-social behaviour societally; developmental psychology describes elements of decision-making and cognition across the formative years. Neuronal connections and release of various neurotransmitters in the brain may reinforce particular behaviours which are further accommodated through the cyberpsychology constructs of online disinhibition, perceived anonymity and online syndication' (Aiken/Davidson/Amann, 2016:8). Not only these **atypical 'organised' offenders** pose a fundamental challenge to the prison system rationale, but also they further illustrate the most relevant question of motivation in cybercrime under the so-called seduction or drift model (Goldsmith/Brewer, 2015). Profit, in addition to other classical criminal motivations – such as moral, political or religious revenge -, are enlarged regarding cybercrime, including reputational gain, mimicking computer game behaviour, intellectual challenge, to impress friends or simply because they have the technology and skills to do it (see Figure 9 in the next page). These mixed motivations pose a crucial problem regarding OC/TN since political aims should be considered along with economic or material profit blurring thereby the divide between them (Basra/Neumann/Brunner, 2016), putting aside the even more thorny question of state or state-sponsored cybercrime, usually overlooked by literature (Broadhurst et al., 2014).

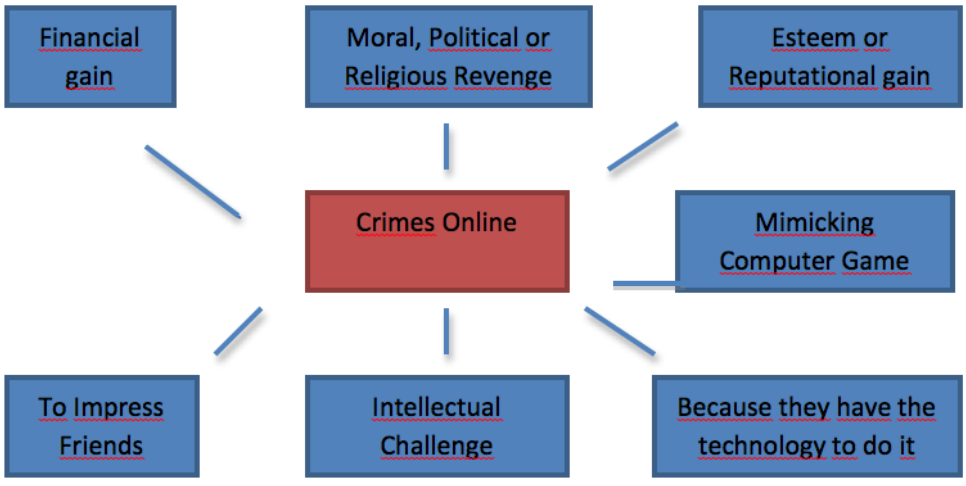


Figure 10. Motivations for organized cyber-crime and cyber-terrorism. Source: Wall (2017) TAKEDOWN Deliverable 2.2

Literature has also delved into the **internal structures of cybercrime groups**. A useful categorisation commonly used is due to McGuire that mentions three types according to offending online, on- and offline and mainly offline, each one divided into two groups depending on their cohesion and command structure. Those are swarms, hubs, extended hybrids, clustered hybrids, aggregates and

hierarchies (McGuire, 2012). Some have linked those group types with different offences (Broadhurst, 2014). Wall has shown that these groups are mostly ephemeral and changes in their small composition are frequent and responsive to new circumstances. They are organised in flat-networked structures, lacking central command but showing anyway a detailed division of labour with specific skill sets. They are bound by the crime, but many are **distributed** affinity groups, formed around 'affinities', shared interests or common goals and '**assemblage'** is a better way to describe how the various cells relate to each other (Wall, 2015). Thus, 'the organisation of crime online follows a different logic to both organised crime and also the organisation of crime offline (…) it is by comparison to the paradigm, a ***dis-organised model*'** (ibid.:85, italics added). However loose these groups may appear and therefore difficult to be qualified under the traditional features of OC (including corruption, violence and so forth), their actions can be premeditated and carefully planned and executed and may cause deep social harm. This has made some authors to reject the applicability of 'organised' paradigm (assumed to be a catch-notion for crime seriousness and dangerousness) in cyberspace (Leukfeldt/Lavorgna/Kleemans, 2016).

Those insights are extraordinary relevant since they demonstrate that cyberspace is not actually 'policeable' and therefore **law enforcement** cannot be the only answer, but also **prevention** and **mitigation** of their impact. That is why **cybersecurity** retains utmost importance and a private-public approach remains unavoidable. Truly, regulation – including criminalization - by hard law instruments has rightly superseded the original international soft-law approach (Segura-Serrano, 2015; UNODC, 2013), the European region being a ground-breaking and leading actor – from the Council of Europe 2001 Budapest Convention on cybercrime to the recent **Directive 2016/1148** on security of network and information systems (NIS directive) (OJ L 194, 19.7.2016). However, being cybercrime global in nature, legal measures need to be coupled with **multi-dimensional** preventative and responsive measures to cyber disruptions and attacks as acknowledged by the EU Cybersecurity Strategy[24]. This inevitably implies a **public-private cooperation** and, by the same token, a **multi-stakeholder** approach. This is particularly important from the European perspective of securing a technologically strong autonomous supply chain, since the European cybersecurity market is too fragmented and different national regulations hinder competitive solutions on a global scale (Olesen, 2016).

However, it should remain, as mentioned earlier, that the cyber dimension works both ways, and it equally opens an extraordinary avenue of possible tools for fighting online and offline both forms of criminality (OC/TN). TAKEDOWN project has undertaken a collection of **Digital Security Solutions** (DDS) with incentivised interest in those present within the European security industry in line with the EU Global Strategy established lines (so far 163 out of 172) that will be available in future **TAKEDOWN Platform**. DDS are defined, in a broad comprehensive spirit, as 'electronic technologies that generate, store, and process data for producing knowledge to be employed by law enforcement agencies (LEAs) –and civilian State's security agencies – to prevent or respond to organised criminal activities and terrorism' (Bonfanti, 2017:10). This definition still encompasses a great variety of technologies ranging from sensors for physical surveillance to algorithms for mining the web. The notion includes both technologies that have been natively designed/conceived for a specific purpose in the context of preventing and fighting crime and terrorism, and technologies serving a more general purpose but that can be used by LEAs (or State's security agencies) to cope with the two phenomena. The collected DSS are being classified according to intended final user ('targeted

[24] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, High Representative and European Commission, Brussels, 7.2.2013, JOIN(2013) 1 final.

customer') (Figure 10) and to its national or international reach, country origin, language available, functionality, applicability to OC, TN or both and (Figure 11).

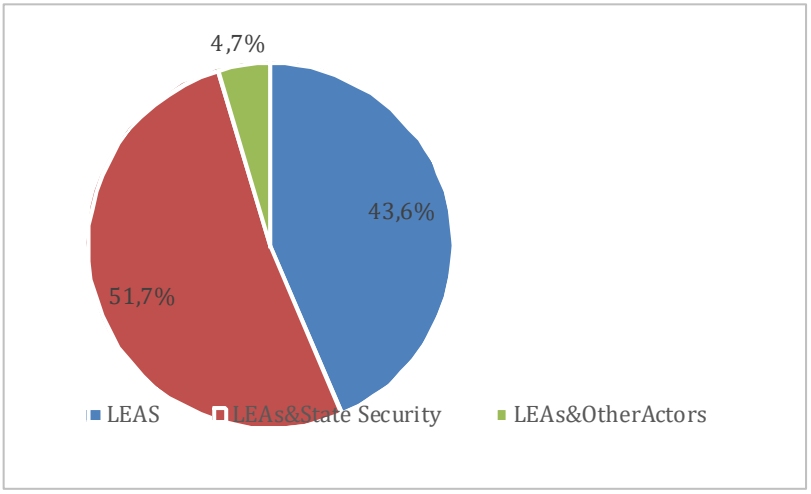


Figure 11. Distribution of DSSS per targeted 'customer'. Source: Bonfanti (2017) TAKEDOWN Deliverable 2.5

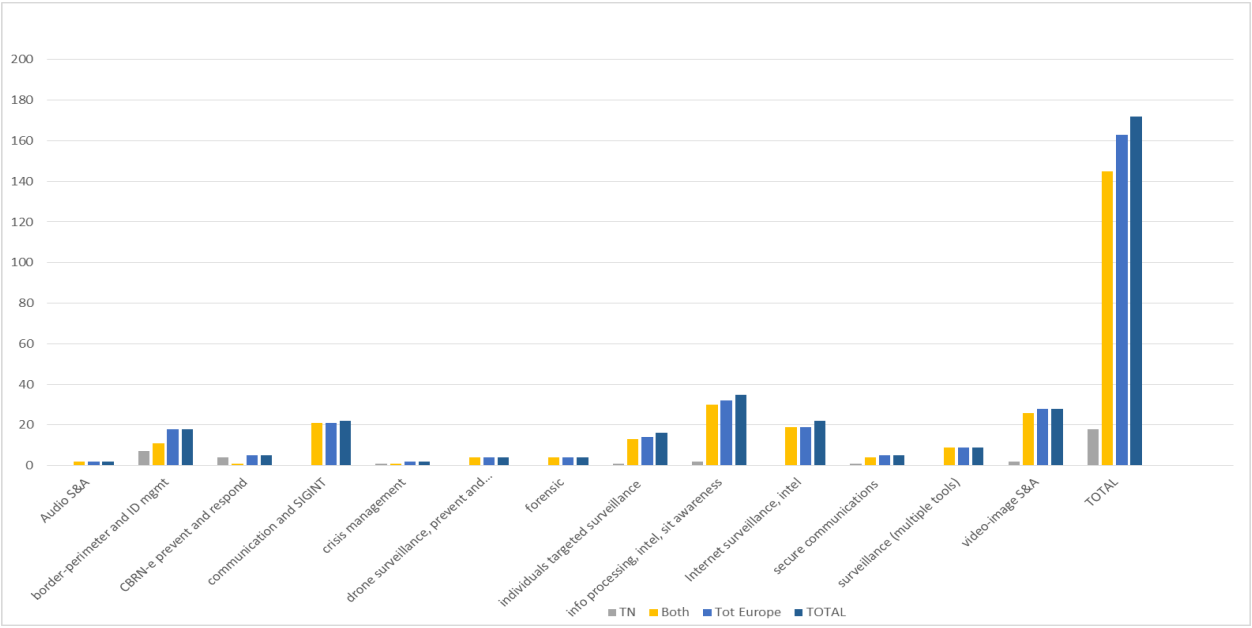


Figure 12. Representation of DSSS per function or field of application.
Source: Bonfanti (2017) TAKEDOWN Deliverable 2.5

4. Conclusion: Methodological Framework for Modelling Organised Crime and Terrorist Networks from TAKEDOWN's Perspective

As the TAKEDOWN-oriented screening of literature shows in Section 3, the various academic disciplines, practice groups and institutions with an interest in organised crime groups and terrorist networks have each developed their own models for understanding and explaining them. These models vary according to the paradigms of the respective disciplines and practices of the groups involved and their different theoretical and methodological approaches. Many of them tend to be rather one-dimensional since often only focused upon one side of the problem, or they lack further usability or transferability towards more practical applications or even may be self-serving. Nevertheless, what those models show by themselves is the need to adopt a methodological framework for modelling OC/TN so that the resulting model could, to the possible extent, overcome those challenges, i.e. that it could convey so many different insights coming from the varied disciplines as well as the complexities that the latter have pointed up. This is the main purpose of this Baseline report in Task Force 2, which is only one step within the Working Plan of TAKEDOWN Project. Then, this methodological framework for modelling OC/TN should be distinguished from the future TAKEDOWN model that will be designed.

The departing point for this methodological modelling framework lies in the need to reflect the fact that OC and TN are socially shaped, but also the complexities that they currently manifest as to their varied evolving structures, their blurred boundaries and un-hermetic aims as well as the multi-faceted countering response that they have given rise to. In other words, it should encompass *the social shaping of OC/TN in a changing socio-political and socio-technical environment where the different structures and the variety of organisational forms through which OC and TN express power (i.e. achieve their goals) can be analysed, connected, cross-referenced and evaluated by all (primary and secondary) stakeholders in order to design strategies, policies, measures and tools to take OC and TN down* (Wall, 2017).

In order to grasp the social shaping of OC/TN Bourdieu's (1990) division between 'field' and 'habitus' is helpful so as to illustrate the variables which define the settings that locate the actors and also shape their actions. The field is the setting which locates agents and determines their status or social capital and it would include (a) the actors who rationally cooperate to commit criminal and terrorist acts, (b) the physical or virtual networked structures that connect these actors and (c) the criminal activities these actors are involved in which impact upon victims and society. The habitus is the way group culture and personal history shape social action, i.e. reflects the lived reality to which individuals are socialized, their individual experience and objective opportunities. Consequently, it involves: (a) society, (b) Government/governance structures and agencies of actors, and (c) public discourse, e.g. the media presents 'truths' and which shapes opinions. By simply listing these six variables, many of the conundrums, complexities, dimensions or even uncertainties that have arisen along these pages find accommodation. That is the case of the public response to OC/TN, the social impact that OC/TN have on society and its perceptions, the threat assessment or the cyber dimension. They also serve to identify which variables out of the six are the different models (and also the scientific perspectives) looking into or explaining their interactions or, if you like, the different interfaces they contribute to understand. Thus, the very methodological challenge for this framework is to be able to accommodate as many as possible of these interfaces, if not all.

This ambition is translated into the six methodological directions to be met by the model or models that TAKEDOWN will deliver, namely (a) handling uncertainty; (b) reflecting dynamic processes; (c) holistic but target-oriented – universally adaptational; (d) open and self-learning; (e) self-reflective and structurally sensitive and (e) fundamental rights abiding. The first three are structural requirements of the model, the following two relate to the functioning of the model, while the last one is normative in character.

Model requirement	Level	Effect(s)
Operational under uncertainty	structural	expand user horizon
Dynamic-friendly	structural	avoid reification methodological indistinctiveness
Universally adaptational	structural	multi-stakeholder friendly target-oriented
Self-learning	functional	cross-fertilization ongoing reassessment
Self-reflective	functional	structural sensitiveness social embeddedness
Fundamental rights abiding	normative	legitimacy social acceptance

Table 8. TAKEDOWN methodological modelling framework

(a) **Operational under uncertainty**

OC/TN have evolved to an extraordinary level of uncertainty, and therefore, the model should be able to manage that uncertainty. OC/TN may adopt many different structures and new distributed criminal networks have emerged. Furthermore, impure hybridization is a relatively established fact; therefore the model has to be responsive to the different aims that criminal or terrorist groups may have endorsed. Beyond that, motivations in criminal actors have expanded to include new ones, which does not go without consequences in preventive and responsive action. In addition radicalisation ending in terrorism encompasses a non-deterministic progression where societal, group and individual factors are as assorted as pertinent, and for that reason the pathways followed may differ greatly from each other.

As a result of the uncertain reality that the model intends to apply, those uncertain variables should be internalized and part of its structure. Conventional as unconventional scenarios should equally be envisioned by TAKEDOWN model, allowing its users to enlarge the possibilities of intervention in the case they are facing in terms of investigative, disrupting or prosecuting purposes. The same applies to preventive intervention to the full extent.

(b) Dynamic-Reflecting

TAKEDOWN model should properly reflect that OC/TN consist of processes and not 'things'. Diagrammatical models are valuable, but in reducing the information flow, they risk **reification**, i.e. they may turn into an un-reflexive 'thing' in the minds of both the reader and practitioner when seeking to apply the model (von Lampe, 2003). Instead, TAKEDOWN model should be able to define patterns of organisation, criminal activities, transaction types, drivers of crime and modus operandi (criminal methods) as processes. The way this will be accomplished is part of Task Force 4. However, from a methodological point of view, this entails a twofold requirement. In the first place, the model should be designed as to internalise any flow of information, which, in systemic terms, means that its

frontiers or borders are porous to the extreme or, in analytical terms, that there must be no discerning or discriminating criteria to be applied for any information to be used by the model. In the second place, this means that the model unit is actually a process, of either prevention, pursue, protection or response.

It should be noted that this feature results in a **methodological indistinctiveness**, which means that no scientific methodology is by definition preferred by the model. Sociological, psychological, socio-psychological or any other are not tested outside the very model. The effectiveness or suitability of those different approaches (which the report has briefly reviewed) is determined by their performance inside the model. This is the methodologically correct, if not only, answer to the indisputably multidimensional character of OC and TN.

(c) Universally adaptational

TAKEDOWN model should correspond to the holistic approach that has been established to tackle OC/TN. In concrete terms, the model has to be **operational for any stakeholder involved**, including the public, so it has to be universal in that regard. It should be remember that the interrelations between the stakeholders might be very different according to the national context. However, the model is to respond to the specific needs of a concrete stakeholder in order to define his/her strategy, policy, measure or tool. In this regard, TAKEDOWN model should be **'target-oriented'** in the sense that the user (a concrete stakeholder) should be able to find a response to the specific quest. Maybe it is worth noting that this target-oriented does not necessarily mean, although it does not exclude it, that only individual cases are handled or processes through the model. As said, process is the unit, whether it is de-radicalising a young right-wing extremist or designing an effective policy or regulation enhancing cybersecurity.

(d) Self-learning

This feature of the model, as said, relates to the functioning of the model and it is the natural consequence of its operation under an open flow of information. The identification of best practices, effective intervention or relevant variables is tested on an on-going basis, so the model itself works in a learning progression. A best practice may be effective in a given case, but later proved ineffective in another one because of a variable not previously present. The identification of stakeholders interested or involved in OC/TN is in itself subjected to the same learning process, as secondary stakeholders might be upgraded to primary ones or introduced for a certain hypothesis.

It should be reminded that the structural features (a), (b) and (c) composed a cross-reference-enabling model open to innovation and, if needed, rectification. This seems particularly convenient in a field, such as fighting OC/TN that are essentially characterised by specific national approaches. In this sense, a natural effect of the model is cross-fertilization and ongoing performance evaluation. Data-mining techniques as any other investigative or anticipatory tool or device for law enforcement, or again preventive action in radicalisation are particularly benefited by this modelling framework that enables ex ante contrasting different national approaches and ex post assessment. This methodological framework requirement directly connected to the social impact assessment regarding counter-terrorism policy and fighting OC. It assures that unintended consequences are detected and re-introduced into the model.

(e) Self-reflective

The second functional feature is also the functional consequence of the structural features (a), (b) and (c), since the model cannot operate oblivious to context. This is translated into structural

sensitiveness. Along the report, structural conditions have emerged once and time as relevant factors in understanding OC/TN and designing effective responses. From a systemic point of view it means that the model relocates itself at any simple time, since it works on a particular structural ground or it is able to self-redimensionate in a case of structural changes. This methodological framework will show its utility in particular in protection society against OC/TN. As protection measures or strategies tend to reduce social vulnerabilities, it is compulsory that the model be able to take these changes into account. If OC/TN are socially shaped, any viable model should be structurally sensitive, i.e. aware of social changes. The emergence of new social norms (e.g. the Addio Pizzo movement) or the enactment of new regulations (e.g. in money-laundering, corruption or cybersecurity) have an undisputed impact on how OC or TN perform and TAKEDOWN model will be able to reflect it.

(f) Fundamental Rights Abiding

Finally, TAKEDOWN model needs to be responsive to the serious concerns that OC/TN poses in terms of compliance with fundamental rights. Good practices, policy guidelines, general or practical preventative measures cannot be endorsed by TAKEDOWN model under any circumstances. The need to introduce this normative requirement is well grounded. There is no doubt that OC/TN are in its own right serious encroachments on fundamental rights and consequently public response must decisively follow. However, this public countering response must stay within the limits that the full respect of fundamental rights draws, where its legitimacy lies. Effectiveness cannot trump legitimacy. This normative alert is fully justified because of the fundamental rights sensitiveness that tackling OC/TN possess from both individual and collective perspective. Increasing incrimination, mass surveillance mechanisms, sensitive information-sharing or multi-stakeholders involvement may well be justified and necessary in preventing, pursuing, protecting from or responding to OC and TN, but it cannot be denied that those policy-legal strategies and/or operational devices are extremely delicate and that they can only apply if they pass a fundamental rights compliance screening.

This normative requirement is applicable in two different sets. On the one hand, TAKEDOWN model itself should operate in full respect of fundamental rights and data protection rights in particular. The scrupulous respect of the Privacy Impact Assessment (PIA) laid down in TAKEDOWN Deliverable 2.2 should guarantee this fulfilment. On the other hand, when functioning, the model should include a fundamental rights alert system in disposition to both raising concerns on particular practices, measures or policies that might encroach on fundamental rights –or require specific assurances-, and automatically rejecting those practices, measures or policies which would infringe upon them with a high degree of certainty. This normative requirement is perfectly in line with the Charter of fundamental rights of the European Union, the European Convention on fundamental rights and the constitutional traditions common to all MS, therefore no measure, digital and non-digital security solution or practice infringing upon them can be allocated or shared by TAKEDOWN model, let alone justified. In those other cases where this conclusion does not reach certainty, for example because national standards differed or there is no clear European case law thereon, this should be unmistakably indicated.

5. References*

Abbas, T. and Awan, I. (2015). Limits of UK Counterterrorism Policy and Its Implications for Islamophobia and Far Right Extremism, *International Journal for Crime, Justice and Social Democracy*, 4: 16-29, available at https://www.crimejusticejournal.com/article/view/241.

Ahmed, S. (2015). The Emotionalization of the War on Terror: Counterterrorism, Fear, Risk, Insecurity and Helplessness, *Criminology & Criminal Justice*, 15: 545-560.

Aiken, M. P. (2016). *The Cyber Effect*, New York: Random House Spiegel & Grau.

Aiken, M., Davidson, J. and Amann, P. (2016) *Youth Pathways into Cybercrime*, Research funded by Paladin Capital Group, https://www.mdx.ac.uk/__data/assets/pdf_file/0025/245554/Pathways-White-Paper.pdf

Albanese, J. S. (2008). *Criminal Justice*. New York: Pearson/Allyn and Bacon.

Albanese, J. S. (2011). *Organized Crime in Our Times*, 6th Ed, New York: Routledge.

Alosi, S. (1983). *Banca e latifondo nella Sicilia degli anni Trenta*. Vol. 100. Naples: Guida Editori.

AlHayat (2014). AlHayat Media Center, Al-Ghuraba - Abu Muslim from Canada, propaganda video released on 12 July 2014.

Andreano, R. and Siegfried, J. (eds) (1980). *The Economics of Crime*, New York: John Wiley.

Arlacchi, P. (1983). *La mafia imprenditrice*, Bologna: Il Mulino.

Armao, F. (2000). *Il sistema mafia. Dall'economia-mondo al dominio locale*, Turin: Bollati Boringhieri.

Baccara, M. and Bar-Isaac, H. (2008). How to organize crime. *The Review of Economic Studies*, 75(4): 1039-1067, available at http://apps.olin.wustl.edu/faculty/baccara/crimeRES.pdf.

Basra, R., & Neumann, P. R. (2016). Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus. *Perspectives on Terrorism*, 10(6): 25-40.

Basra, R., Neumann, P. and Brunner, C. (2016). Criminal Pasts, Terrorist Futures: European Jihadists and the New Crime-Terror Nexus, ICSR King's College London, http://www.icsr.info.

Beare, M. (2010). Women and Organized Crime, Report No. 13/2010, Research and National Coordination Organized Crime Division, Law Enforcement and Policy Branch, Public Safety Canada, available http://publications.gc.ca/site/archivee-archived.html?url=http://publications.gc.ca/collections/collection_2012/sp-ps/PS4-106-2010-eng.pdf

Beccaria, C. (1965 [1765]). *Dei delitti e delle pene*, Turin: Utet.

Beck, C.J. (2016). *Radicals, Revolutionaries and Terrorists*, Cambridge: Polity.

Bentham, J. (1967 [1776]). *A Fragment of Government. With an Introduction to the Principles of Morals and Legislation*, Oxford: Basil Blackwell.

Berry, N., Ko, T., Moy, T., Smrcka, J., Turnley, J., & Wu, B. (2004, July). Emergent clique formation in terrorist recruitment. In *The AAAI-04 Workshop on Agent Organizations: Theory and Practice*. http://www.aaai.org/Workshops/ws04.php

Bianchi, S. (2017). Screen Current Organised Crime and Terrorist Networks Response Approaches, Initiatives, Strategies and Policies in Europe, TAKEDOWN Deliverable 2.4

Black, D. (2004). The Geometry of Terrorism, *Sociological Theory*, 22: 14-25.

Block, A. (1991). *Perspectives on Organizing Crime. Essays in Opposition*, Dordrecht: Kluwer.

Block, A. A., & Chambliss, W. J. (1981). *Organizing crime*. New York: Elsevier.

Blum, G. and Heymann, P.B. (2010). *Laws, Outlaws and Terrorists*, Cambridge: MIT Press.

Bonfanti, M. (2017). TAKEDOWN Deliverable 2.5.

Borum, M. (2011). Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research, *Journal of Strategic Security*, 4(4), 37-62, available at https://www.researchgate.net/publication/254706697_Radicalization_into_Violent_Extremism_I_A_Review_of_Social_Science_Theories.

Bourdieu, P. (1990). Structures, habitus, practices. *The logic of practice*, 52-65, available at https://monoskop.org/images/8/88/Bourdieu_Pierre_The_Logic_of_Practice_1990.pdf.

* All references include an open source when it is available, except for official documents that are open-access at the official websites. All the links have been last accessed on 28 June 2017.

Brenner, S. (2006): Cybercrime, cyberterrorism and cyberwarfare. *Revue internationale de droit pénal*, 77(3-4): 453-471, available at: http://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-453.htm

Broadhurst et al. (2014). Broadhurst, R., Grabosky, P, Alazab, M. and Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, *International Journal of Cyber Criminology* 8(1): 1-20, available at http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf.

Buc, P. (2015). *Holy Wars, Martyrdom and Terror*, Philadelphia: University of Pennsylvania Press.

Calderoni, F. (2008). A Definition that Could not Work: the EU Framework Decision on the Fight against Organised Crime, *European Journal of Crime, Criminal Law and Criminal Justice*, 16(3): 265-282, author's version available at https://publicatt.unicatt.it/retrieve/handle/10807/1575/95230/Calderoni - A definition that could not work - the EU FD on OC - AAM.pdf.

Calderoni, F. (2010). *Organized Crime Legislation in the European Union. Harmonization and Approximation of Criminal Law, National Legislations and the EU Framework Decision on the Fight Against Organized Crime*, Heidelberg: Springer.

Campana, P. (2016). Explaining criminal networks: Strategies and potential pitfalls. *Methodological Innovations*, 9: 1-10, available at http://journals.sagepub.com/doi/pdf/10.1177/2059799115622748.

Campana, P. and Varese, F. (2012). Listening to the wire: criteria and techniques for the quantitative analysis of phone intercepts. *Trends in organized crime*, 15(1): 13-30.

Campana, P. and Varese, F. (2013). Cooperation in criminal organizations: Kinship and violence as credible commitments. *Rationality and society*, 25(3): 263-289.

Campbell, L. (2014). Organized Crime and National Security: A Dubious Connection?, *New Criminal Law Review* 17(2): 220-251, available at http://dro.dur.ac.uk/19860/.

Carnegie Commission (1997). *Preventing Deadly Conflict: Final Report*, The Carnegie Corporation of New York, available at http://www.carnegie.org/publications/preventing-deadly-conflict-final-report.

Carrapico, H. (2014). Analysing the European Union's responses to organized crime through different securitization lenses, *European Security*, 23(4): 601–661.

Carrapico, H. and Lavorgna, A. (2015). Space Oddity? Exploring Organised Crime Ventures in Cyber Space, Special issue editorial, *The European Review of Organised Crime*, 2(2): 1-5, available at http://sgocnet.org/site/wp-content/uploads/2014/07/00_Editorial_pp1-5.pdf.

Cesoni, M. L. (2017). Le droit européen anti-terroriste : notes en marge d'une fuite en avant, *Cahiers de la sécurité et de la justice*, 38: 61-71.

Chazan, G. and Atkins, R. (2016). Twelve killed as truck ploughs into Berlin Christmas market, *Financial Times*, https://www.ft.com/content/557b9bbe-c626-11e6-8f29-9445cac8966f

Chermac, S.M., Freilich, J.D. and Caspi, D. (2010), 'Policy Makers and Law Enforcement Must Consider the Unintended Consequences of Their Proposed Responses to Extremist and Terrorist Groups', in Frost, N.A., Freilich, J.D. and Clear, T.R. (eds), *Contemporary Issues in Criminal Justice Policy*, Belmont: Wadsworth, 139- 150.

Chin, K. L., and Godson, R. (2006). Organized Crime and the Political Criminal Nexus in China, *Trends In Organized Crime*, 9(3): 5-44.

Cloward, R. And Ohlin, L. (1960). *Delinquency and Opportunity*, New York: The Free Press.

Cohen, A. (1955). *Delinquent Boys: The Culture of the Gang*, New York: The Free Press.

Cohen, J. and Blanco, J. M. (2016). Knowledge, the Great Challenge do Deal with Terrorism, *Revista de Estudios en Seguridad Internacional*, 1(1): 43-62, available at http://www.seguridadinternacional.es/revista/?q=content/knowledge-great-challenge-deal-terrorism.

Combs, L. (2013). *Terrorism in the Twenty-First Century*, London: Pearson.

Cressey, D. (1969). *Theft of the Nation: The Structure and Operations of Organized Crime*, New York: Harper & Row.

D'Angelo, E. and Musumeci, M. (2016). Organized Crime and the Legal Economy. The Italian Case, Turin: United Nations Interregional Crime and Justice Research Institute (UNICRI), available at http://files.unicri.it/UNICRI_Organized_Crime_and_Legal_Economy_report.pdf.

De Andrés, A. P. (2008). West Africa under attack: drugs, organized crime and terrorism as the new threats to global security, *UNISCI Discussion Papers*, 16, available at https://www.ucm.es/data/cont/media/www/pag-72513/UNISCI DP 16 - Andres.pdf.

De Boer, J. and Bosetti, L. (2015). The Crime-Conflict 'Nexus': State of the Evidence, *Occasional Paper 5*, United Nations University Centre for Policy Research, July 2015, available at http://collections.unu.edu/eserv/UNU:3134/unu_cpr_crime_conflict_nexus.pdf.

De Londras, F. and Doody, J. (Eds). *The Impact, Legitimacy and Effectiveness of EU Counter-terrorism*, London: Routledge. A previous version within the SECILE project is available at https://fdelondras.files.wordpress.com/2016/01/secile-d5-3.pdf.

Decker, S. and Pyrooz, D. (2011). Gangs, Terrorism, and Radicalization, *Journal of Strategic Security*, 4(4): 151-166, available at http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1145&context=jss.

Dino, A. and Pepino, L. (eds) (2008). *Sistemi criminali e metodo mafioso*, Milan: Franco Angeli.

Dino, A. and Ruggiero, V. (2012). Il metodo mafioso, *Studi sulla Questione Criminale*, special issue, VII (1): 1-130.

Downes, D. and Rock, P. (1988). *Understanding Deviance. A Guide to the Sociology of Crime and Rule Breaking*, Oxford: Clarendon Press.

Durkheim, E. (1996). *Professional Ethics and Civic Morals*, London: Routledge.

Dzhekova, R. et al (2016). Understanding Radicalisation: Review of Literature, Center for the Study of Democracy, Sofia, available at: http://www.csd.bg/artShow.php?id=17560

EB86 (2016). Public Opinion in the EU. First Results, Standard Eurobarometer 86, Autum 2016.

Eeckhout, P. and López Escudero, M. (eds) The European Union's External Action in Times of Crisis, Oxford: Hart Publishing.

Edwards, A. (2016). Actors, Scripts, Scenes and Scenarios: Key Trends in Policy and Research on the Organisation of Serious Crimes, *Oñati Socio-legal Series [online]*, 6 (4): 975-998. Available from: https://ssrn.com/abstract=2875318.

Edwards, A. and Levi, M. (2008). Researching the Organization of Serious Crime', *Criminology and Criminal Justice*, 8 (4): 363-388, available at https://www.researchgate.net/publication/249786378_Researching_the_organization_of_serious_crimes.

EMCDDA (2010). The State of the Drugs Problem in Europe: Annual Report, Lisbon: EMCDDA.

EMCDDA (2016). European Drug Report 2016: Trends and Developments, Lisbon.

EMCDDA/Europol (2016). European Drug Markets Report: Strategic Overview, Lisbon/The Hague.

English, R. (ed) (2016). *Illusions of Terrorism and Counter-Terrorism*, Oxford: Oxford University Press.

EUCTC (2016). State of play on implementation of the statement of the Members of the European Council of 12 February 2015, the JHA Council Conclusions of 20 November 2015, and the Conclusions of the European Council of 18 December 2015, Brussels, 4 March 2016, Council of the EU 6785/16.

European Central Bank (2011). Biannual Information on Euro Counterfeiting, Brussels, 17 January.

European Commission (2016). *Towards a single EU VAT area – Time to decide*, Brussels, COM (2016) 148 final.

Europol (2011a). EU Organised Crime Threat Assessment, The Hague: Europol Public Information.

Europol (2011b). Knowledge Report: Trafficking in Human Beings in the European Union, The Hague: Europol Public Information.

Europol (2015). Exploring Tomorrow's Organised Crime, The Hague.

Europol (2016a). European Union Terrorism Situation and Trend Report 2016, The Hague.

Europol (2016b). Changes in modus operandi of Islamic State terrorist attacks. Review held by experts from Member States and Europol on 29 November and 1 December 2015, The Hague.

Europol (2016c). Internet Organised Crime Threat Assessment, The Hague.

Europol (2017a). EU Serious and Organised Crime Threat Assessment. Crime in the ages of technology, The Hague, Europol Public Information.

Europol (2017b). European Union Terrorism Situation and Trend Report 2017, The Hague.
Europol/OHIM (2015). 2015 Situation Report on Counterfeiting in the European Union. A joint project between Europol and the Office for Harmonization in the Internal Market.
Fellman, P. (2015). Modeling Terrorist Networks: The Second Decade, In Fellman, P., Bar-Yam, Y. and Minai, A. (eds) *Conflict and Complexity: Countering Terrorism, Insurgency, Ethnic and Regional Violence*, New York: Springer, 3-34.
Ferreira, O. R. (2016). Violent Mexico: Participatory and Multipolar Violence Associated with Organized Crime, *International Journal of Conflict and Violence*, 10(1): 41-60, available at http://www.ijcv.org/index.php/ijcv/article/view/395/pdf.
Fijnaut, C. (1990). Organized Crime: A Comparison Between the United States of America and Western Europe, *British Journal of Criminology*, 30(3): 321-40.
Fijnaut, C. and Paoli, L. (eds) (2004). *Organised Crime in Europe*, Dordrecht: Springer.
Freilich, J., Chermak, S.M. and Gruenewald, J. (2015). The Future of Terrorism Research, *International Journal of Comparative and Applied Criminal Justice*, 39 (4): 353-369.
Gambetta, D. (1992). *La mafia siciliana. Un'industria della protezione privata*, Turin: Einaudi.
Gambetta, D. (1996). *The Sicilian Mafia: the business of private protection*. Boston: Harvard University Press.
Gambetta, D., and Reuter, P. (1995). Conspiracy among the many: the mafia in legitimate industries. In *The Economic Dimensions of Crime*, London: Palgrave Macmillan, 99-120
Gilmour, S. (2015). Policing Crime and Terrorism in Cyberspace: An Overview *The European Review of Organised Crime*, 2(2): 143-159, available at http://www.sgocnet.org/site/wp-content/uploads/2014/06/EROC119.pdf.
Goldsmith, A. and Brewer, R. (2015). Digital drift and the criminal interaction order, *Theoretical Criminology*, 19(1) 112-130, available at http://journals.sagepub.com/doi/pdf/10.1177/1362480614538645.
González, A. L., Freilich, J. D. and Chermak, S. M. (2014). How Women Engage Homegrown Terrorism, *Feminist Criminology*, 9(4): 344-366.
Gottfredson, M. and Hirschi, T. (1990). *A General Theory of Crime*, Stanford: Stanford University Press.
Gounev, P. and Ruggiero, V. (eds) (2012). *Corruption and Organized Crime in Europe*, London: Routledge.
Grabosky, P. and Stohl, M. (2010). *Crime and Terrorism*, Thousand Oaks: SAGE.
Hassner, R.E. (2016). *Religion on the Battlefield*, Ithaca: Cornell University Press.
Herlin-Karnell (2013). From Mutual Trust to the Full Effectiveness of EU Law: 10 Years of the European Arrest Warrant, *European Law Review*, 38(1): 79-91.
Horkuc, H. (2009). *Said Nursi: Makers of Islamic Civilization*, Oxford: Oxford University Press.
House of Lords (2016). Brexit: future UK-EU security and police cooperation, 7th Report of Session 2016–17, *HL Paper 77*, December 2016, London.
Iacolino, S. (2013). Report on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report), Special committee on organised crime, corruption and money laundering, European Parliament, (2013/2107(INI).
Ianni, F. (1972). *A Family Business. Kinship and Social Control in Organized Crime*, New York: Russell Sage Foundation.
IEP (2016). *Global Terrorism Index 2016. Measuring and Understanding the Impact of Terrorism*, New York: Institute for Economics & Peace.
Illes, A. et al (2014). *Understanding the damages of environmental crime. Review of the availability of data*, http://www.efface.eu
Jacobs, B.J. and Wyman, E.D. (2015). 'Organized Crime Control in the United States of America', in Paoli, L. (ed), *The Oxford Handbook of Organized Crime*, Oxford: Oxford University Press.
Jordán Enamorado, J. (2015). Incidencia del terrorismo de inspiración yihadista en Estados Unidos y Europa Occidental: un análisis comparado, *Revista Española de Ciencia Política*, 37: 89-117, available at http://www.ugr.es/~jjordan/Terrorismo yihadista en Europa y Estados Unidos.pdf.
Kefauver Committee (1951). *Report on Organized Crime*, New York: Didier.

Kennedy, H. (2016). *The Caliphate*, Harmondsworth: Pelican.

Koops B.-J. (2016). Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research, in Akhgar, B. and Brewster, B. (eds), *Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities*, Springer International Publishing Switzerland, 3-15.

Krebs, V. E. (2002). Mapping networks of terrorist cells. *Connections*, 24(3): 43-52, available at http://vlado.fmf.uni-lj.si/pub/networks/doc/seminar/krebs.pdf.

Kruglanski, A.W. et al (2009). 'Fully Committed: Suicide Bombers' Motivation and the Quest for Personal Significance', *Political Psychology*, 30 (3): 331-354.

Kusak, M. (2016). Mutual admissibility of evidence in criminal matters in the EU. A study of telephone tapping and house search, *IRCP Research Series*, Antwerpen, vol. 53, available at https://prawo.amu.edu.pl/__data/assets/pdf_file/0011/326909/IRCP-53-M-Kusak-Mutual-admissibility-E-version.pdf.

LaFree, G., Yang, S-M. and Crenshaw, M (2010). International Cooperation, Not Unilateral Policies May Be the Best Counterterrorist Strategy, in Frost, N.A., Freilich, J.D. and Clear, T.R. (eds), Contemporary Issues in Criminal Justice Policy, Belmont: Wadsworth, 121-128.

Landesco, J. (1969 [1929]). *Organized Crime in Chicago: Part III of the Illinois Crime Survey*, Chicago: University of Chicago Press.

Laqueur, W. (2002). 'Life as a Weapon', Times Literary Supplement, 6: 3-4.

Lavezzi, A. M. (2008). Economic structure and vulnerability to organised crime: Evidence from Sicily. *Global Crime*, 9(3): 198-220, available at https://mpra.ub.uni-muenchen.de/50114/1/MPRA_paper_50114.pdf.

Lavezzi, A. M. (2014). Organised crime and the economy: A framework for policy prescriptions. *Global Crime*, 15(1-2): 164-190.

Lavorgna, A. (2015). Organised crime goes online: realities and challenges, Journal of Money Laundering Control, 18(2): 155-168.

Leukfeldt, E. R., Lavorgna, A. and Kleemans, E. R. (2016). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, *European Journal on Criminal Policy and Research,* DOI: 10.1007/s10610-016-9332-z, https://link.springer.com/article/10.1007/s10610-016-9332-z

Levi, M. (2014). Thinking About Organised Crime: Structure and Threat, The RUSI Journal, 159(1): 6-14, available at http://www.tandfonline.com/doi/full/10.1080/03071847.2014.895253?scroll=top&needAccess=true.

Levi, M. (2016). The impacts of organised crime in the EU: some preliminary thoughts on measurement difficulties, *Contemporary Social Science*, 11(4): 392-402.

Levi, M. and Maguire, M. (2004). Reducing and preventing organised crime: An evidence-based critique. *Crime, Law and Social Change*, 41(5): 397-469, available at https://www.academia.edu/24489424/Reducing_and_preventing_organised_crime_An_evidence-based_critique.

Levi, M. and Maguire, M. (2011). Financial and Organised Crime in Europe: Converging Paradigms of Control?, in Spapens, T., Groenhuijsen, M. and Kooijmans, T. (eds) *Universalis. Liber amicorum Cyrille Fijnaut*. Antwerp: Intersentia, 723-733.

Levi, M., Innes, M., Reuter, P. and Gundur, R. (2013). *The Economic, Financial & Social Impacts of Organised Crime in the EU*, European Parliament, PE 493.018.

Lewitt, M. (2016). Hezbollah's Transnational Organised Crime, *Policy Watch 2609*, The Washington Institute for Near East Policy.

Liñán Nogueras, D. J. (2017). Un nuevo discurso estratégico para la política exterior de la Unión Europea, *Revista de Derecho Comunitario Europeo*, 56: 11-24.

Lodato, S. and Scarpinato, R. (2008). *Il ritorno del principe. La criminalità dei potenti in Italia*, Milan: Chiarelettere.

Lombroso, C. (1894]). *Gli anarchici*, Turin: Bocca.

Lombroso, C. and Laschi, R. (1890). *Il delitto politico e le rivoluzioni*, Turin: Bocca.

Luiijf, E. (2014). New and emerging threats of cyber crime and terrorism, B. Akhgar, A. Staniforth and F. M. Bosc (eds.) *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Walthan: Syngress (Elsevier): 19-29.

Makarenko, T. (2004). 'The Crime-Terror Continuum: Tracing the Interplay Between Transnational Organized Crime and Terrorism', *Global Crime*, 6: 129-145, available at http://www.iracm.com/wp-content/uploads/2013/01/makarenko-global-crime-5399.pdf.

Mangas Martín, A. and Liñán Nogueras, D. J. (2016). *Instituciones y Derecho de la Unión Europea*, 9th ed., Madrid: Tecnos.

Mann, M. M. (2014). A Story of Organized Crime: Constructing Criminality and Building Institutions. PhD thesis, Australian Research Council Centre of Excellence in Policing and Security (CEPS) Griffith University, available at https://eprints.qut.edu.au/91930/

Markov, D., Ilcheva, M. and Yordanova, M. (2017). Collection of stakeholders and key representatives, TAKEDOWN Deliverable 2.3.

Marrero Rocha, I. (2016). Los combatientes "terroristas" extranjeros de la Unión Europea a la luz de la Resolución 2178 (2014) del Consejo de Seguridad de las Naciones Unidas, *Revista de Derecho Comunitario Europeo,* 54: 555-594.

Marrero Rocha, I. (2017). Nuevas dinámicas en las relaciones entre crimen organizado y grupos terroristas, *Revista Española de Derecho Internacional*, forthcoming.

Martín Rodríguez, P. (2016). La emergencia de los límites constitucionales a la confianza mutua en el Espacio de libertad, seguridad y justicia en la sentencia del Tribunal de Justicia *Aranyosi y Caldararu*, *Revista de Derecho Comunitario Europeo*, 55: 859-900.

Martin, G. (2010). *Understanding Terrorism. Challenges, Perspectives and Issues*, Thousand Oaks: Sage.

Mazzitelli, A. L. (2007). Transnational Organized Crime in West Africa: The Additional Challenge, *International Affairs*, 83(6): 1071-1090.

McAfee, R. P., Mialon, H. M. and Williams, M. A. (2004). What is a Barrier to Entry?, *American Economic Review,* 94(2): 461-465, available at http://authors.library.caltech.edu/11284/1/MCAaer04.pdf.

McCauley, C. and Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism, *Terrorism and political violence*, 20(3): 415-433, available at http://www.brynmawr.edu/aschcenter/mccauley/webpage stuff/2008 mechanisms rad McC Moskale.pdf.

McCulloch, J. and Pickering, S. (2009). Pre-Crime and Counter-Terrorism', *British Journal of Criminology*, 49: 628-645, available at http://statecrime.org/data/2011/10/mcculloch2009a.pdf.

McDonald, K. (2013). *Our Violent World. Terrorism in Society*, London: Palgrave Macmillan.

McGuire, M. (2012). *Organised Crime in the Digital Age*, John Grieve Centre for Policing and Security, London.

Merton, R. (1968). *Social Theory and Social Structure*, New York: The Free Press.

Militello V. (2015). Transnational Organized Crime and European Union: Aspects and Problems, in Ruggeri, S. (ed) *Human Rights in European Criminal Law. New Developments in European Legislation and Case Law after the Lisbon Treaty*, Heidelberg: Springer, 201-214.

Mitsilegas, V. (2009). *EU Criminal Law*, Oxford: Oxford University Press.

Mitsilegas, V. (2016). Mutual recognition, mutual trust and fundamental rights after Lisbon, in V. Mitsilegas et al. (eds) *Research Handbook on EU Criminal Law*, Cheltenham: Elgar, 148-168.

Moghaddam, F.M. (2005). The Staircase to Terrorism. A Psychological Exploration, *American Psychologist*, 60(2): 161-169.

Morselli, C. (2009). *Inside criminal networks* (Vol. 8). New York: Springer.

Morselli, C., Gabor, T. and Kiedrowski, J. (2010). The Factors That Shape Organized Crime, Report 7/2010, Research and National Coordination Organized Crime Division, Law Enforcement and Policy Branch, Public Safety Canada, available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rgnzd-crm-brf-7/index-en.aspx

Mueller, J. and Stewart, M. (2016). *Chasing Ghosts. The Policing of Terrorism*, Oxford: Oxford University Press.

Naylor, R. T. (2002). *Wages of Crime: Black Markets, Illegal Finance and the Under-world Economy*, Ithaca: Cornell University Press.

Neumann, P. (2013). The Trouble with Radicalization, *International Affairs*, 89(4): 873-893.

Neumann, P. (2016). Breaking the wall of radicalisation. How Security Studies Explore the Roots of Terror, http://falling-walls.com/videos/Peter-Neumann-10670.

Núñez Noriega, G. and Espinoza Cid, C. E. (2017). El narcotráfico como dispositivo de poder sexo-genérico: crimen organizado, masculinidad y teoría *queer*, *Estudios de Género de El Colegio de México*, 3(5): 90-128, available at http://estudiosdegenero.colmex.mx/index.php/eg/index.

Obokata, T. (2011). Key EU Principles to Combat Transnational Organized Crime, *Common Market Law Review*, 48(3): 801-828.

Oftedal, E. (2015). *The financing of jihadi terrorist cells in Europe*, FFI-rapport 2014/02234, Norwegian Defence Research Establishment (FFI), available at http://www.ffi.no/no/Rapporter/14-02234.pdf.

Olesen, N. (2016). European Public-Private Partnerships on Cybersecurity - An Instrument to Support the Fight Against Cybercrime and Cyberterrorism, B. Akhgar and B. Brewster Eeds.), *Combatting Cybercrime and Cyberterrorism. Challenges, Trends and Priorities*, Springer International Publishing Switzerland, 259-278.

Pantucci, R., Ellis, C. and Chaplais, L. (2015). Lone-Actor Terrorism. Literature Review, Countering Lone-Actor Terrorism Series No. 1, London: RUSI (Royal United Services Institute for Defence and Security Studies), available at http://www.strategicdialogue.org/wp-content/uploads/2016/02/Literature_Review.pdf.

Paoli, L. (2002). The paradoxes of organized crime. *Crime, law and social change*, 37(1): 51-97.

Paoli, L. (ed) (2014). *The Oxford Handbook of Organized Crime*, Oxford: Oxford University Press.

Peers, S. (2016). *EU Justice and Home Affairs Law*, 4th ed., Oxford:OUP, vol. II.

Peterson, M. (1991). The Changes of a Decade, *Criminal Organizations*, 6(3-4): 20-2.

Picarelli, J. T. and Shelley, L. (2002). Methods not Motives: Implications of the Convergence of International Organized Crime and Terrorism, *Police Practice and Research: An International Journal*, 3(4): 305–318.

Polo, M. (1995). Internal cohesion and competition among criminal organizations. *The economics of organised crime*, 87-108.

Poniatowski, G. (Dir) (2016). *Study and Reports on the VAT Gap in the EU-28 Member States: 2016 Final Report*, CASE – Warsaw: Center for Social and Economic Research (Project leader), available at https://ec.europa.eu/taxation_customs/sites/taxation/files/2016-09_vat-gap-report_final.pdf.

Powell, W. (2003). Neither market nor hierarchy. *The sociology of organizations: classic, contemporary, and critical readings*, 315, 104-117.

Propaganda booklet (How to Survive in The West, Mujahid Guide, Propaganda booklet, https://www.investigativeproject.org/documents/misc/863.pdf

Ramadan, H. and Shantz, J. (eds), (2016). *Manufacturing Phobias. The Political Production of Fear in Theory and Practice*, Toronto: Toronto University Press.

Ramalingam, V. (2012). *Far-Right Extremism. Trends and Methods for Response and Prevention,* London: Institute for Strategic Dialogue, available at https://www.academia.edu/2301197/Far-Right_Extremism_Trends_and_Methods_for_Response_and_Prevention.

Ramalingam, V. (2014). *Old Threat, New Approach: Tackling the Far Right across Europe*, London: Institute for Strategic Dialogue, available at https://www.counterextremism.org/resources/details/id/463/old-threat-new-approach-tackling-the-far-right-across-europe.

Reif, E. (2015). Das „Dschihadismus"-Phänomen. Eine Frage der Partizipation?, *Soziales_Kapital. wissenschaftliches journal österreichischer fachhochschul-studiengänge soziale arbeit*. Nr. 14: http://www.soziales-kapital.at/index.php/sozialeskapital/article/viewFile/388/664.pdf]

Reitano, T., Clarke, C. and Adal, L. (2017). *Examining the Nexus between Organised Crime and Terrorism and its implications for EU Programming*, CT-Morse GITOC, Publications, 20 April 2017, http://www.ct-morse.eu/author/ct-morse

Requena, L., de Juan, M., Giménez-Salinas, A. and de la Corte, L. (2014). A psychosocial study on crime and gender: Position, role and status of women in a sample of Spanish criminal

organizations, *Revista de Psicología Social / International Journal of Social Psychology*, 29(1): 121–149, available at http://www.tandfonline.com/doi/full/10.1080/02134748.2013.878572?scroll=top&needAccess=true

Reuter, P. (1983). *Disorganized Crime. Illegal Markets and the Mafia*, Cambridge: The MIT Press.

RHIPTO/Global Initiative Against Transnational Organized Crime (2015). Libya: a growing hub for Criminal Economies and Terrorist Financing in the Trans-Sahara, Policy Brief, Norwegian Center for Global Analysis and Global Initiative Against Transnational Organized Crime, available at http://globalinitiative.net/wp-content/uploads/2015/05/2015-1.pdf.

Ross, J. I. (1993). Structural Causes of Oppositional Political Terrorism: Towards a Causal Model, *Journal of Peace Research*, 30(3): 317-329.

Ruggiero, V. (1996). *Organized and Corporate Crime in Europe: Offers That Can't Be Refused*, Aldershot: Dartmouth.

Ruggiero, V. (2000). *Crime and Markets*, Oxford: Oxford University Press.

Ruggiero, V. (2005). *Understanding Political Violence*, Maidenhead: Open University Press.

Ruggiero, V. (2010a). Armed Struggle in Italy: The Limits to Criminology in the Analysis of Political Violence, *British Journal of Criminology*, 50(4): 708-724.

Ruggiero, V. (2010b). Organised Behaviour and Organised Identity, *Beijing Law Review*, 1: 14-19.

Ruggiero, V. (2012). Introduction: The Organization of Crime, in Gounev, P. and Ruggiero V. (eds), *Corruption and Organized Crime in Europe*, London and New York: Routledge.

Ruggiero, V. and Leyva, R. (2016). Literature exploration and open access bibliography, TAKEDOWN Deliverable 2.1, http://takedownproject.eu.

Ruiz Díaz, L. J. (2015). *La lucha contra el crimen organizado en la Unión Europea. Aspectos internos y dinámicas externas del discurso securitario*, PH Dissertation, University of Granada, http://0-hera.ugr.es.adrastea.ugr.es/tesisugr/25575715.pdf.

Sacks, J. (2015). *Not in God's Name. Confronting Religious Violence*, London: Hodder and Stoughton.

Saviano, R. (2006). *Gomorra*, Milan: Mondadori.

Scarpinato, R. (2004). La storia: Italia mafiosa e Italia civile', *Micro Mega*, 5: 259-286.

Schmid, A. P. (2013). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review, *ICCT Research Paper*, The Hague: International Centre for Counter-Terrorism, available at https://www.icct.nl/download/file/ICCT-Schmid-Radicalisation-De-Radicalisation-Counter-Radicalisation-March-2013.pdf

Scott, J. (1988). Social network analysis. *Sociology*, 22(1): 109-127.

Segura-Serrano (2015). Cybersecurity: towards a global standard in the protection of critical information infrastructures, *European Journal of Law and Technology*, 6(3): 1-24, available at http://ejlt.org/article/viewFile/396/592

Sergi, A. (2015). Divergent mind-sets, convergent policies. Policing models against organised crime in Italy and in England within international frameworks, *European Journal of Criminology*, 12(6): 658-680.

Sergi, A. (2016). National Security vs Criminal Law. Perspectives, Doubts and Concerns on the Criminalisation of Organised Crime in England and Wales, *European Journal on Criminal Policy and Research*, 1-17.

Shelley, L. I. and Picarelli, J. T. (2002). Methods not Motives: Implications of the Convergence of International Organized Crime and Terrorism, *Police Practice and Research*, 3(4): 305-318.

Silke, A. (2008). Holy Warriors: Exploring the Psychological Processes of Jihadi Radicalization, *European Journal of Criminology*, 5: 99-123.

Sinai, J. (2016). A Framework for Assessing the Mobilization of Westerners by Jihadists in Syria and Intervention Points for Counter-Measures. *Perspectives on Terrorism*, 10(3): 45-52, available at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/514/html.

Small, T. (2016). 'Wars of Religion', Times Literary Supplement, 23 September, Middle East Special Feature: 1-12.

Spaaij, R. (2010). The Enigma of Lone Wolf Terrorism: An Assessment, *Studies in Conflict and Terrorism*, 33(9): 854-870, available at

http://www.tandfonline.com/doi/full/10.1080/1057610X.2010.501426?scroll=top&needAccess=true.

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social networks*, 13(3): 251-274, available at http://hbanaszak.mjr.uw.edu.pl/TempTxt/PDF/Sparrow_1991_TheApplicationOfNetworkAnalysisToCriminalIntelligence.pdf.

Stigler, G. J. (1968). Barriers to entry, economies of scale, and firm size. *The Organization of Industry*, 67-70.

Toboso, M. (2017). 2016: escenario negro... ¿en regresión?, *Análisis GESI*, 2017/1, Granada, available at http://www.seguridadinternacional.es/?q=es/content/2016-escenario-negro…-¿en-regresión.

Toscano, R. (2016). Il tempo della paura, *Micro Mega*, 2: 119-128.

UNODC (2010). World Drug Report, Vienna: UNODC.

UNODC, (2012a). Report: The use of the Internet for terrorist purposes, Vienna: UNODC.

UNODC (2012b). Compendio de casos de delincuencia organizada. Recopilación comentada de casos y experiencias adquiridas, New York: United Nations.

UNODC (2013). Comprehensive Study on Cybercrime, Vienna: UNODC.

UNODC (2016). Global Report on Trafficking in Persons 2016, Vienna: UNODC.

Van Ginkel, B. and Entenmann, E. (eds) (2016). The Foreign Fighters Phenomenon in the European Union. Profiles, Threats & Policies, *ICCT Research Paper*, The Hague: International Centre for Counter-Terrorism, available at https://icct.nl/wp-content/uploads/2016/03/ICCT-Report_Foreign-Fighters-Phenomenon-in-the-EU_1-April-2016_including-AnnexesLinks.pdf.

Varese, F. (2001). *The Russian Mafia: Private Protection in a New Market Economy*, Oxford: Oxford University Press.

Varese, F. (ed) (2010a). *Organized Crime: Critical Concepts in Criminology*, London: Routledge.

Varese, F. (2010b). *What is organised crime?* New York: Routledge.

Varese, F. (2011). *Mafias on the move: How organized crime conquers new territories*. Princeton: Princeton University Press.

Veldhuis. T. and Staun, J. (2009). *Islamist Radicalisation: A Root Cause Model*. The Hague: Netherlands Institute of International Relations Clingendael, available at https://www.diis.dk/files/media/publications/import/islamist_radicalisation.veldhuis_and_staun.pdf

Vidino, L. (2011). *Radicalisation, Linkage and Diversity: Current Trends in Terrorism in Europe,* Santa Monica: RAND.

Von Lampe, K. (2003). The use of models in the study of organized crime. In *Proceedings of the 2003 Conference of the European Consortium for Political Research (ECPR)*, Philipps-Universitat Marburg, 18-21 Sept, available at http://www.organized-crime.de/kvlECPRocmodels.pdf.

Von Lampe, K. (2006). The interdisciplinary dimension of the study of organized crime, *Trends in Organized Crime*, 9(3): 77-94 [an author's version is available at http://www.organized-crime.de/kvlInterdiscDimStudyOC-TOC-9-3-2006.pdf].

Von Lampe, K. (2008). Organised Crime in Europe: Conceptions and Realities, *Policing: A Journal of Policy and Practice*, 2(1): 7-17[an author's version is available at http://www.organized-crime.de/KlausvonLampeOCEuropePolicing2008.pdf].

Von Lampe (2013). Recent Trends in the Study of Transnational Organized Crime, *Fan zui yan jiu (Chinese Criminology Review)*, 33(3):89-97 [available in English at http://www.academia.edu].

Von Lampe, K. (2016). Organized Crime. Analyzing Illegal Activities, Criminal Structures, and Extra-Legal Governance, Thousand Oaks: Sage.

Von Lampe, K. and Ole Johansen, P. (2004). Organized Crime and Trust: On the conceptualization and empirical relevance of trust in the context of criminal networks, *Global Crime*, 6(2): 159-184, available at https://www.researchgate.net/publication/248955491_Organized_Crime_and_Trust_On_the_conceptualization_and_empirical_relevance_of_trust_in_the_context_of_criminal_networks.

Wall, D. S. (2007). *Cybercrime: the transformation of crime in the information age*, Cambridge: Polity Press.

Wall, D. S. (2015). Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime, *The European Review of Organised Crime*, 2(2): 71-90, available at https://www.academia.edu/16517486/Dis-organised_Crime_Towards_a_Distributed_Model_of_the_Organization_of_Cybercrime.

Wall, D. S. (2017) Modelling Organised Crime Groups and Terrorist Networks, TAKEDOWN Deliverable 2.2.

Wang, P. (2013). The Rise of the Red Mafia in China: A Case Study of Organised Crime and Corruption in Chongqing, *Trends in Organized Crime*, 16(1): 49-73.

Whiteside, C. (2016). 'New Masters of Revolutionary Warfare: The Islamic State Movement (2002-2016)', *Perspectives on Terrorism*, 10: 6-20, available at http://www.terrorismanalysts.com/pt/index.php/pot/article/view/523/html.

Williams, P. (2001). Transnational criminal networks, in J. Arquilla and D. Ronfeldt (eds) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND, 61-96.

Williams, P. (2002). Cooperation Among Criminal Organizations, M. R. Berdal, M. Serrano (eds), *Transnational Organized Crime and International Security: Business as Usual?*, London: Boulder, 67-80.

Wills, G. (2016). 'My Koran Problem', New York Review of Books, 16-19.

Witte, R. (1996). *Racist Violence and the State*, London: Longman.

Yordanova, M. and Markov, D. (2012), Countering Organised Crime in Bulgaria: Study on the Legal Framework, Center for the Study of Democracy, Sofia, available at: http://www.csd.bg/artShow.php?id=16048

Yordanova et al. (2014). Yordanova, M., Markov, D. and Ilcheva, M., Report and factsheet on prevalence of cybercrime and related enforcement activity, S. Maffei, and L. Markopoulou (eds) (2014) *FIDUCIA: New European Crimes and Trust-based Policy*. Volume 2, available at: http://www.fiduciaproject.eu/media/publications/12/FiduciaV2_web.pdf

Young, J. K. (2016). *Measuring terrorism, Terrorism and Political Violence*, DOI: 10.1080/09546553.2016.1228630, available at http://www.tandfonline.com/doi/full/10.1080/09546553.2016.1228630?scroll=top&needAccess=true

Zöller, M. A. (2012). Verschwimmende Grenzen zwischen Terrorismus und Organisierter Kriminalität, in Sinn, A. and Zöller, M. A. (ed) *Neujustierung des Strafrechts durch Terrorismus und Organisierte Kriminalität*, Heidelberg: C.F. Müller, 1-14.

6. List of Figures

7. List of Tables