CHALLENGES AND AVAILABLE SOLUTIONS AGAINST ORGANIZED CYBER-CRIME AND TERRORIST NETWORKS

ANDREA TUNDIS[1], FLORIAN HUBER[2], BERNHARD JÄGER[2], JÖRG DAUBERT[1], EMMANOUIL VASILOMANOLAKIS[1] & MAX MÜHLHÄUSER[1]
[1]Department of Computer Science, Technische Universität Darmstadt, Darmstadt, Germany
[2]SYNYO, Vienna, Austria

ABSTRACT

Organized Crime (OC) and Terrorist Networks (TN) have risen to major and persistent threats for the European Union and its population. The IT growth of the past decade caused a migration of OC/TN to the cyber domain as well as the introduction of cybercrime. As a consequence, the technological dimensions of criminal activities are becoming more relevant and challenges ranging from the identification of criminal activities up to the understanding of engagement processes, are even more complicated. In this context, this paper aims to provide a discussion on OC and TN by pointing out organizational models, similarities, distinguishing features and differences in terms of their objectives. Furthermore, the main issues and available categories of solutions, in terms of models, methods and software tools are described. Finally, the importance of innovative digital and non-digital solutions is discussed as well as the current research directions are highlighted.

Keywords: Cybercrime, cyber security, cyber terrorism, organized crime, terrorist networks.

1 INTRODUCTION

Criminality has always been a big problem in everyday life of people. Especially nowadays it represents one of the major and persistent threats for the European Union and its population [1–3]. Criminality can be distinguished into two main branches: *Organized Crime* (OC) that is typically aimed at achieving economic and financial goals; whereas *Terrorist Networks* (TN), whose goals are usually driven by moral, social and religious interests. Unfortunately, due to the rapid evolution of mass media, social networks and generally of the Internet, even more illegal activities take place in the virtual domain [4]. Indeed the Internet offers a wide spectrum of activities and possibilities, which can be abused for OC/TN purposes. As a consequence, the technological dimension of criminality is becoming even more relevant and dangerous.

The modern society is surrounded by systems and services that are mostly build in terms of physical, mechanical, and electrical systems which in turn are closely linked and controlled by ICT infrastructures [5]. Even the media, which are massively used for advertising purposes, have radically evolved and become more dynamic and interactive. On one hand, this brings benefits in terms of the well-being of life through the use of more effective services ranging from sending messages, transferring money, tele-medicine and so on, worldwide in real time. On the other hand, if used maliciously they can represent a great threat to humanity. In fact, through their improper use, it is possible to (i) launch attacks and compromise at far distance industries, factories, systems and so on (ii) threaten people; (iii) advertise illegal activities, sell drug via dark markets, etc.

Due to the high degree of activity distribution at the individual level, which is enabled by such technologies, the fighting process is getting more difficult. Consequently, it is necessary to identify what the main problems are, and get increased awareness regarding the functioning of such criminal systems. Having a better understanding, it is important to solve challenges ranging from (i) identification of criminal activities; (ii) understanding of

WIT Transactions on The Built Environment, Vol 174, © 2018 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE170391

engagement processes; (iii) improving the communication among citizens, specialists and law enforcement agencies [6, 7]. In this panorama, the paper provides an overview about OC and TN by providing a view of the current state of the art in terms of main challenges, available solutions, current needs and possible research directions in the European context.

The rest of the paper is structured in the follow way: Section 2 describes in more detail Organized Crime and Terrorist Networks by highlighting the main characterizing aspects and differences; in Section 3, the most important Criminal organization models and crime typologies are reported; whereas the major open issues are discussed in Section 4. Some of the most related available solution in terms are described Section 5, whereas the current research directions are introduced in Section 6. Finally, conclusions are drawn in Section 7.

2 ORGANIZED CRIME VS TERRORIST NETWORKS

The base of terrorism and crime is the corruption [8]. Highly corrupted societies give little room for the development and growth of other societies. Under these circumstances, the lesser employment opportunities for the youth, forces them to find alternative paths to succeed which may also lead towards the criminality. Organized crime and terrorist networks may share connected by three aspects: *Coexistence, Cooperation and Convergence* [1]. Specifically:

- *Coexistence*, because they may concurrently occupy and operate in the same geographical area;
- *Cooperation*, because they may try to reach their objectives and threatening the society by working together;
- *Convergence*, because typically one starts operating in the direction which is associated with the other.

There is no single definition for Organized Crime [9], and typically it involves a minimum of two people working together [10]. In the modern society its definition has a broader concept according to the range of action, that can focus on financial target or other source of gain by exploiting IT technology. In this later case, we talk about cyber-crime which differs from physical crime in four ways: it is easier to commit, it requires minimal resources for potential damage, it can be committed in a jurisdiction where the criminal is not physically present and it is not always considered completely illegal [11]. With the help of information and communication technologies, criminals easily operate across borders [9]. In fact, today most of the organized crime is done by skilled technicians who apply their knowledge in criminal activities. These are those conventional crime groups who had started to harness digital technology in committing crimes [12]. Organized criminals had adopted more-networked structural models, internationalized their operations and grown more technologically [6]. Nowadays, most of the criminal organizations are capable of performing cyber crime and they can be a highly structured group that attracts delinquent IT professionals. They can organize either a small group for a short project or a complete community that operates on-line. It may also consist of individuals who operate alone but still linked to a criminal network or networks that can be found in other specific sub-network. Conventional organized crime groups are increasingly involving in digital crime. Today these groups with global reach are harming consumers, business and government interests on daily basis. The technology has helped these groups by reducing national trade barriers, widen transportation infrastructure and support volumes of international trade. Smugglers took advantage from growing international commerce to hide their illegal trade and integrated financial system allowed them to move their profits globally to any place. Organized groups are becoming more market focused and adopting to changes in legal and illegal economies.

Table 1: Organized crime and terrorist networks: main distinguishing features.

Characteristics	OC	TN
Focus on getting money quickly, easily and efficiently by illegal activities	Yes	No
Mostly hide their identity and work anonymously	Yes	No
Do things to get media attention	No	Yes
Attack citizens and infrastructure	No	Yes
Bring harm and fear among citizens	Yes	Yes
Bring political change by their activities	No	Yes
Can engage in each other activities	Yes	Yes
Depends on external network or support	Yes	No
Using information technology for performing their activities	Yes	Yes
Adaptive and change their actions according to market changes	Yes	No

Furthermore, these groups are involved in criminal activities such as trafficking (drugs trafficking, human trafficking etc.) and money laundering, but they are increasingly involving themselves in high-tech less traditional crimes which hides their identities, forge of goods and other types of frauds.

Terrorist Networks (TN) are also becoming bigger and increasingly dangerous. The network consist of different components as the command nucleus, field cell, group communication, national host, sympathizers and support assets which all together combines and make a TN [13]. TN have various characteristics such as low signal to noise ratio (sparse relevant observations), geographic distribution, dynamic and adaptive structure [14]. Such groups capitalize and invest also in advanced technologies to find newer and easier ways to engage youth by exploiting social media, on-line videos, channels, websites and chat rooms [15]. These phenomena are unfortunately growing, and the way of doing it is changing. TN are getting more sophisticated in performing their operations, especially in terms of technology. The use of cyber space is becoming a force multiplier for their objectives including: elaborate ideological propaganda campaign, radicalization and recruitment of new followers and educating them on topics ranging from data analysis up to use of explosives [16]. TN are also able to perform cyber-terrorism through cyber attacks and compromise the national security of a country by using computer networks to shut down critical infrastructure and coerce civilian population or even intimidate the government [17].

As described above OC and TN, are very different criminal organizations, especially in terms of objectives and way of acting. A summary of their distinguishing features is depicted in Table 1.

3 ORGANIZATIONAL MODELS IN CRIMINAL ORGANIZATIONS

Understanding and interpreting human and social behavior is one of the biggest challenges to be faced. This aspect becomes even more complicated when rules and actions change according to the reference system. In fact, in OC and TN specific behaviors and actions are dictated by the environment, and in particular by considering types of crimes, targets and criminal organizational models. From their combinations is defined who can do what and to what extent. For example, the organizational model establishes the structure and powers assigned to each member, as a consequence, based on the level of power within a certain structure, a member is empowered to a certain type of crime. Criminal Organizational models are very complicated, and they can be characterized by many dimensions such as: structure, size, activities, trans-border operations, identity, violence, corruption, political influence and penetration into the legitimate economy. By considering for example their organization from a structural point of view the following four type of hierarchies represented in Fig. 1 are the most recurrent [18].

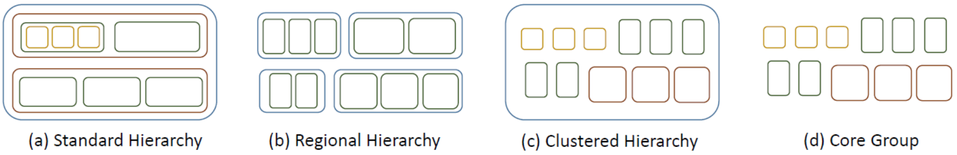
(a) Standard Hierarchy (b) Regional Hierarchy (c) Clustered Hierarchy (d) Core Group

Figure 1: Structural organizations.

In particular, a description of each of the structures is give below:

- *Standard hierarchy:* this is the most common form of criminal groups. There is a leader, who has a strong internal control over other members and there is a chain of members with clearly defined roles of individual. This is a top down hierarchy in which, the leader has complete discipline over its members by sending orders. Members of this kind of group have similar background which helps them to coordinate with each other.
- *Regional hierarchy:* regional hierarchy has similar characteristics with standard hierarchy. Indeed such structures have a chain of members and command as well as strong internal discipline and distinct roles in the group. The main difference between them is the decentralization of power, which allows local or small organizations to work and control over a particular geographical region. It also allows the small and local groups to engage in different criminal activities and spread their geographic region which helps to increase transnational criminal activities.
- *Clustered hierarchy:* in this kind of hierarchy, criminal groups are independent and perform their activities autonomously. They operate and are controlled up to a certain extent under a centralized body. These small groups' coordination depends upon the association they have with each other in performing various activities. Like regional hierarchy, it allows small groups to engage in different criminal activities and widen their geographical region.
- *Core Group:* core groups are very small groups and this makes them very disciplined in nature. These small groups are surrounded by a large network of linked members and are unstructured in nature. All members of these groups have equal share of power and control and they are very hard to track because of no social identity and working behind a legitimate business run by other groups.

The above mentioned models become more complicated when other aspects are considered such as social aspects, relationships, reputation among ”families”. Examples of such models are for example the *Bureaucratic model* and the *Patrimonial (Patron-Client) model:*

- *Bureaucratic models:* these kinds of models (such as the Italian American criminal organization) have very generic characteristics as they have a single leader at the top and lower levels consist of different members with individual role defined. This group works similar to government organizations and every activity is conducted with the approval of higher authority. These models consist of three main components: Family-like structure with ranks of authority from the boss down to the soldiers; bosses oversee the activities of the ”family” members and a commission of bosses handle inter-family relations and disputes.

- *Patrimonial models:* this is a family network model and relies on the relationships in families, friends and financier. It grows by recruiting family members and an example of this kind of model organization is Sicilian mafia. It comes under the category of social models and has social and cultural ties between each other.

Some other criminal organizations can be very flexible and can take place for temporary or specific purposes. They are defined as *Criminal Network* which contains individuals who are recruited and work for a well-defined job. These group members unite for an ongoing task and are not necessarily connected to each other socially. They are very adaptable in nature and allow them to reform a group after the task is complete. This individual skills and combination of resources provide them advantage in trafficking activities. This kind of networks can have different organizational structures. The most common are: (i) *Directed network:* this model works like hierarchical network but it is formed for a specific activity by the core leaders. (ii) *Mesh network:* these models are self organized and decentralized in nature. Members perform tasks with other members without the need of any leader. (iii) *Transactional network:* these models are completely dependent on brokers or middlemen, who are responsible for transaction between entities. (iv) *Flux network:* these models are very small, unstable in nature and have very small established structure. Members usually do not trust each other or they have a very little trust which is easy to break.

4 MAJOR ISSUES IN EUROPEAN COMMUNITY

As discussed so far the world of the criminality has many faces, which makes things very complex to be understood and solved. As a consequence, this Section restricts the focus by discussing the most relevant issues that have been investigated in the European context. An important discriminating element, considered in this analysis, is the IT part, which has led to the identification of two main categories of issues named hereinafter as: *Basic Issues*, and *Advanced Issues*. In particular, the former issues do not specifically involve technological aspects and they are mainly raised by differences and divergences among Member States of the European Union (EU), whereas the latter lay strongly their foundations on the IT technology growth. In the following sub-sections both these categories are presented.

4.1 Basic issues

It is widely accepted that dealing with OC and TN requires help and cooperation among states, companies and the inner state system in the global regulation of the internet [19]. Unfortunately, the theory sometimes differs from practice, because of cultural, ethical, religious, and historical reasons that make their convergence difficult to be reached. This is the typical European scenario based on a community built around states with different background. Indeed, many gaps exist due to the differences and divergences among the member atates which, in turn, raise important issues. Fig. 2, shows the major societal problems identified at European level [4]: *Low Level of Cooperation, Weak Communication Mechanisms, Inconsistency among National and International Laws, Absence of Citizens' involvement*.

Low Level of Cooperation. It can be perceived at different organization levels and it exists due to the lack of cooperation and trust among police forces, law enforcement agencies,

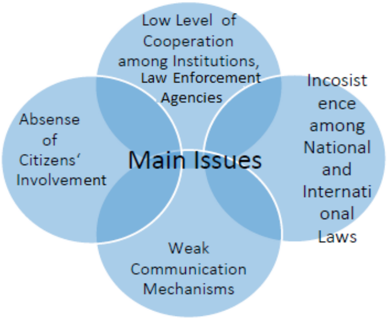
Low Level of Cooperation among Institutions, Law Enforcement Agencies
Incosistence among National and International Laws
Absense of Citizens' Involvement
Main Issues
Weak Communication Mechanisms

Figure 2: Main issues.

as well as among national governments. This phenomenon can be observed, since nations provide hardly data of their citizens for their analysis, which could be useful for detecting suspicious activities. Furthermore, if from one side, different efforts have been conducted, among states in terms of signed treaties, to prevent criminalities; from the other side their implementation is still weak.

Weak Communication mechanisms. This issue derives partially from the previous one. Communication and notification mechanisms represent a very important aspect to counteract illicit activities. Unfortunately, most of the authorities get to know about the crime very late and it becomes difficult to stop the malicious activity and to track the criminals. As a consequence, the improvement of communication and notification mechanisms play a relevant role to prevent the risk of attacks, as well as to reduce the effect of damage, especially in terms of loss of human lives.

Inconsistency among National and International Laws. The lack of a uniform and coherent legislative system among member states is the cause of many faults, which often allow criminals to pursue their goals without too much troubles. There are multiple legislative frameworks but no single organization has the authority over all. Indeed, there are cases in which some activities are considered legal in some countries and illegal in others, thus leading to conflict at a legal level, allowing criminals to commit crimes by exploiting legal gaps.

Absence of Citizens' Involvement. If on the one hand, the person's damage is the primary target of criminal activities, then the people represents the most important and powerful weapon to fight criminality. Unfortunately, their involvement is still weakly considered. Specific programs devoted to citizens, which aim to create greater awareness among people and that enable them to support the authorities in the fight against crime, are not really taken into account yet.

The aforementioned issues represent the main vulnerabilities, which have been currently identified, in the EU context. Starting from them and by exploiting more sophisticated tools, new issues and illegal activities have emerged, as it is discussed in the next sub-section.

4.2 Advanced issues and emerging illegal activities

As highlighted in Section 4.1, some fundamental gaps exist among Member States. Based on such inconsistencies, further problems emerge, especially favored by the use of computer tools. Indeed, the main enabling factors, related to the IT growth, rely in:

- *Dematerialization of Illegal Activities:* thanks to the exploitation of the Internet, it is no more necessary to be physically in a specific place to commit a crime, to threaten a person, to steal money, or to sell drugs or weapons;
- *Increased International Collaborations:* it is easier to get in touch with other people, establish new contacts and relationships, as well as to organize illegal activities and improve collaborations with foreign criminal organizations;
- *Online Anonymity:* it is in highly exploited by criminal groups which put them outside the capacity of law enforcement and intelligence organizations. In fact, criminals are able to hide their identities by using specific techniques to coordinate activities across borders (e.g. to send encrypted messages) which allows them not to expose themselves.

Based on such factors, even well-known issues become difficult to solve with well-established solutions due to such technological factors, for example the *identification* represents a primary problem. For instance, well-known illegal activities (such as drug sales) are evolving, and becoming complicated to be localized in the virtual space. This is due to a lack of technological tools, innovative methods, as well as adequate resources and skilled staff. A typical example is represented by a Cold Boot attack, that is used by authorities to get the key of encrypted hard disks [20]. Usually criminals use Tor Browser to hide their identity and specific method of full disk encryption [21]. In order to catch a hacker and to obtain some proofs against him, a specific kind of process, called Cold Boot attack, can be followed. Unfortunately, only few countries or agencies have in-house professionals with these kind of expertise who are able to conduct such analysis.

Among the wide set of emerging illegal activities, or those that are digitally evolving thanks to the exploitation of the IT growth, the most popular are for example [22–24]: *Steganography*, a communication technique used for hiding secret messages inside other messages or pictures; *Money laundering and Black Market*, a electronic payment mechanism used by criminals and terrorist organizations to remain undetected; *Tumbler algorithms*, it is used to transfer money from one place to another by exploiting bots, which in turn, attempt to break links between transactions and send money by dummy transactions series. Furthermore, the *Darknet*, which is conceived as a network of hosts/computers not indexed by search engines where the participants interact anonymously, it is exploited by the crime organization or terrorist network to perform illegal peer to peer sharing. *Botnets*, a cyber criminal tool which is created with malicious software known as malware. It transforms a computer into a bot and allows performing automated tasks on the Internet without being controlled by the rightful user.

These and many other problems are nowadays enabled from the IT growth. Those make criminals free to act, by exploiting the current authorities limitations, especially in terms of IT-skills, that make them unprepared to deal with Organized Crime and Terrorist Networks in the cyber space.

5 CATEGORIES OF AVAILABLE SOLUTIONS

Fighting the modern criminality is not a trivial task, rather it requires huge efforts to identify the right aspects to be faced, the way to deal with them and then to define or adopt the proper solutions. Different proposals already exist in literature, some of them have been natively conceived for specific purposes, some others are general purposes, which in turn could be reused or even customized to be exploited in the context OC and TN. They can be grouped into three main categories: *Models*, *Methods and Approaches*, *Cyber tools and Service*s (see Fig. 3), which are described in the following sub-sections.

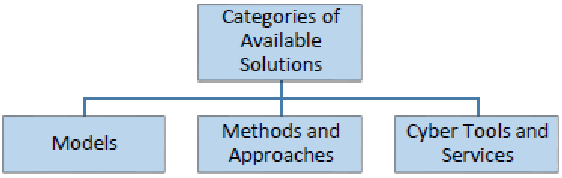

Figure 3: Main categories of available solutions.

5.1 Models

To identify a solution, typically the first useful tool is the definition of a *model*, which is used to represent the phenomenon under consideration to be analyzed. Many research efforts are devoted to the definition and employment of Models that are exploited to represent a particular aspect of interest of the real world to be studied. Indeed, models are build by identifying the concepts of reference domain in order to define a common terminology/vocabulary as well as relationships among them. Then specific information/data is customized according to the objectives to be reached. In the traditional studies of criminal activities the most popular models are centered on [4, 25, 26]:

Radicalization Awareness Network (RAN): this model helps to bring together experts and practitioners from around the world and facilitates the exchange of ideas on concerned topics. RAN works against radicalization and also posting online videos to counter negative videos.

End point detection and response model: such a model deals with solutions focusing on detection, investigating and mitigating issues with hosts and endpoints. It is used to monitor and analyze the state of the end points for detecting indications of suspicious activities so as to be able to react in short time.

Continuous monitoring: this kind of model helps to effectively detect, contain and eradicate an attack. It monitors the outgoing traffic to suspicious sites, also searches for effected machines within the network and analyzes if sensitive data has been compromised or not. This can be done by various tools like malware detection tools, netflow data analysis, Argus software, SILK and so on.

Digital forensics: this model constitutes the use of scientifically derived and proven methods towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal.

Risk based security model: this helps in proper risk assessment by the companies and to turn both security breach data and vulnerability intelligence into information, and information into a competitive edge to address security risks.

Cyber crime treaty as symbolic legislation: this model comprises of four functions that are as follows: (i) Function of reassuring public, which ensures public that the law makers are making tough decisions on crime and terrorist activities; (ii) Moral educative function, which constitutes educating people about right and wrong behavior concerning the Internet in all countries; (iii) Function as model for other states. Countries with no previous laws pertaining to cyber crime or had outdated laws; this model is acting as a learning model for them; (iv) Function as deterrent future criminal behavior.

5.2 Methods and approaches

Other solutions are more focused on the exploitation of methods, approaches and techniques. These solutions are based on well-defined processes and best practices for supporting the analysis of dynamic aspects and changes that may occur in the system under consideration. Examples of such categories of solutions are described below [14, 27, 28].

Anomaly Detection: it can be used to find fraudulent financial transactions which can be used to perform illegal or terror activities. For example, it is used to detect fraud in credit card purchases or illegal transfer of money from one place to other.

Steganalysis: it is an analysis techniques which is exploited to identify hidden data under the cover of media files. For example, it is used against Steganography to find hidden data under image, audio and video files.

Social Network Analysis (SNA): it is a technique to analyze social networks on the basis of social relationships. It works by using nodes (actors) in social network and finding the relationships between them. In OC/TN, it is used for predicting/identifying suspicious activities as well as to recognize key players, leaders, activity patterns and communication patterns.

Sentiment Analysis (SA): it refers to the use of natural language processing, text analysis, computational linguistics, and biometrics to systematically identify, extract, quantify, and study affecting states and subjective information. SA aims to determine the attitude of a subject with respect to some topic or the overall contextual polarity or emotional reaction to a document, interaction, or event.

Adaptive Safety Analysis and Monitoring tool (ASAM): it is used by organizations to identify terrorist threats, predicting possible terrorist actions and elucidating ways to counter terrorist activities. It is mainly based on Hidden Markov models, Bayesian networks, Petri nets, colored diagrams and it operates by identifying relationships between data and observing transactions and changes.

Geographical Information Systems (GIS): it is technique that works with monitoring and surveillance for predicting four important aspects: when, where, how and who. It uses various sources for information such as public service agencies, homeland security systems and intelligence department for producing the results. It helps in preventing, predicting and counter terrorist activities based on Monitoring, Preparedness, Response and Mitigation stages.

Spatial Event Analysis: this is an analysis technique employed as a decision support tool for confronting terrorist organizations. The goal of this technique is to provide real and accurate visualization of terrorist networks. It is based on GIS to identify pattern and pattern changes. It also produces information about area of operation, modus operandi and it provides information on the growth of the area of the terrorist network.

5.3 Cyber tools and services

The third category of solutions is represented by digital solutions. They are implemented to make processes more efficient by automating them or by supporting humans into making decisions. Two main categories of digital solutions have been identified in this context: *Public Security Services (PSS)* and *Cyber Security Solutions (CSS)*.

- *PSS* are represented by *helplines*, *info-lines*, *reporting platforms*, *information hubs*, and *contact points* [29–31]. Such services are used to support the public and citizens in case of risk or danger. From one side, they provide listening and emotional support to anyone in situation of distress via telephone or interactive chats; whereas from the other side they are exploited to report suspicious activities.

- *CSS* are represented mainly by tools that might be employed by LEAs, Polices forces and so on to prevent/counter OC/TN [32–34]. They are based both on electronic technologies that generate, store, and process data for producing knowledge, as well as on technologies ranging from sensors for physical surveillance up to algorithms for mining which are suitable to prevent or respond to organized criminal activities and terrorism.

6 ONGOING RESEARCH DIRECTIONS

As above described, TN and OC are threats that have always existed, and they are continuously evolving. As the technology evolves also the issues change, as a consequence, new challenges have to be faced by exploiting proper tools. That is why tradition solutions and approaches are no longer effective in the information era for fighting and to prevent the modern criminality.

Furthermore, most of the approaches, available in literature, are limited to the analysis of information expressed in the English language, as discussed in [35]. To cover the issues related to multi-cultural and international aspects highlighted in Section 4, strong attention is currently devoted towards the definition of a model that allows textual analysis by taking into account meta-data concerning the geo-location, the language as well as any information related to the country of origin, religion, gender, etc. As a consequence, there is need for more flexible, dynamic and cyber solutions able to support the human activities, not only exploitable from domain experts but also easily accessible to the citizens.

On the basis of the studies conducted in the context of European Research project TAKEDOWN [36], the current efforts are evolving towards semiotic solutions [37]. Semiotic is the science that studies the life of signs within the society. This is important because in addition to analyzing text, identify topics, other complementary information need be to considered such as cultural aspects, location, religion, language and so on [38]. By exploiting such approach, the current research directions are devoted to (see Fig 4):

- *Identification of suspicious users* and related activities on the web, as it is considered the main means of communication and venue of illegal activities.

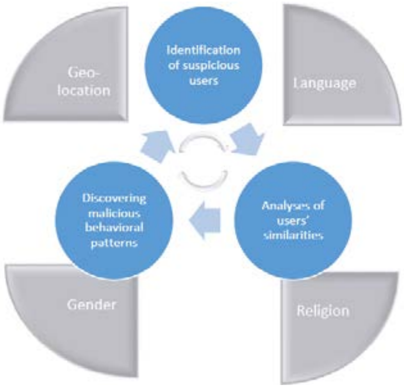
Geo-location
Identification of suspicious users
Language
Discovering malicious behavioral patterns
Analyses of users' similarities
Gender
Religion

Figure 4: Ongoing research directions.

- *Analysis of user similarities* in order to identify on-line collaboration and network among groups of criminals
- *Discovering malicious behavioral patterns* which can be used to predict and suppress premeditated malicious attacks.

7 CONCLUSION

The paper dealt with criminal activities by giving an overview on Organized Crime and Terrorist Networks. In particular, it provided an overview about the main characterizing aspects as well as the main differences between them. Then a description among the main organizational models in criminal organizations were provided, by highlighting the most common typologies of crime and organizational models. Afterwards, the main issues with particular reference to the EU context were identified and discussed by distinguishing between basic and advanced ones, enabled by the IT growth. The current status of available solutions classified in models, methods and approaches, cyber tools and services were presented. Finally, due to the current shortcomings, the importance of innovative and more effective cyber tools were highlighted, by briefly introducing the current activities, future perspectives and research directions in the context of the TAKEDOWN research project.

ACKNOWLEDGMENT

The work in this paper is performed in the context of the TAKEDOWN research project, which receives funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement no 700688.

REFERENCES

[1] Alda, E. & Sala, J.L., Links between terrorism, organized crime and crime: the case of the Sahel Region. *Stability: International Journal of Security and Development*, **3**(1), 2014.
[2] Chistyakova, Y. & Wall, D.S., *Organised Crime in the United Kingdom*, 2015.
[3] Savona, E. U. & Riccardi, M. (eds), From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. *Final Report of EU Co-funded Project OCP – Organised Crime Portfolio*, 2015.
[4] Marion, N.E., The Council’s of Europe Cybercrime Treaty: An exercise in Symbolic Legislation. *International Journal of Cyber Criminology*, vol. 4(2), pp. 699–712, 2010.
[5] Anil, A., Kumar, D., Sharma, S., Singha, R., Sarmah, R., Bhattacharya, N. & Singh, S.R., Link prediction using social network analysis over heterogeneous terrorist network. *IEEE International Conference on Smart City*, Chengdu (China), Dec. 19–21, 2015.
[6] Bjelopera, J.P. & Finklea, K.M., Organized crime: an evolving challenge for U.S. law enforcement. *Congressional Research Service*, 2012.
[7] European Commission, *Preventing Radicalization to Terrorism and Violent Extremism: Strengthening the EU’s Response*, 2014.
[8] Shelley, L.I., Organized Crime, Terrorism and Cybercrime, *Security Sector Reform: Institutions, Society and Good Governance*, Eds. Alan Bryden and Philipp Fluri, 2003.
[9] Brady, H., The EU and the fight against organized crime, *Center for European Reform*, 2007.
[10] Rickards, C., What are the barriers to gathering and sharing organised crime intelligence: an Australian perspective. *The European Review of Organised Crime*, **3**(1), 2016.

[11] Aseef, N., Davis, P., Mittal, M., Sedky, K. & Tolba, A., *Cyber-Criminal activity and analysis*, 2005.

[12] Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S., Organizations and cyber crime: an analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology*, **8**(1), 2014.

[13] Smith, R., Counter terrorism simulation: a new breed of federation. *Simulation Interoperability Workshop*, Spring, 2002.

[14] Allanach J., Tu, H., Singh, S., Willett, P. & Pattipati, K., Detecting, tracking and counteracting terrorist networks via hidden Markov models. *IEEE Aerospace Conference*, 2004.

[15] The European Commission, preventing radicalization to terrorism and violent extremism: strengthening the EU's response. *IEEE Aerospace Conference*, 2014.

[16] Doyle, H., New Tools, new vulnerabilities: the emerging cyber-terrorism dyad. *Cyber Defense Review*, 2015.

[17] Lewis, J.A., Assessing the risks of cyber terrorism, cyber war and other cyber threats. *Center of Strategic and International Studies*, Washington, DC, 2002.

[18] Le, V., Organised Crime typologies: structure, activities and conditions. *International Journal of Criminology and Sociology*, pp. 121–131, 2012.

[19] Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J. & Scherrer, A., Fighting cybercrime and protecting privacy in the cloud, *European Parliament, Directorate-General for Internal Policies, Policy Department*, 2012.

[20] Halderman, J.A., Lest we remember: cold-boot attacks on encryption keys. *ACM Communication*, **52**(5), pp. 91–98, 2009.

[21] Raab, J. & Milward, H.B., Dark networks as problems. *Public Administration Research and Theory*, **13**(4), pp. 413–439, 2003.

[22] Bojarski, K., Dealer, hacker, lawyer, spy. modern techniques and legal boundaries of counter-cybercrime operations. *The European Review of Organised Crime*, 2015.

[23] Sui, D., Caverlee, J. & Rudesil, D., The deep web and the Darknet: A Look inside the Internet's massive block, *Eds. Wilson Center*, 2015.

[24] Wilson, C., Botnets, Cybercrime, and Cyber-terrorism: Vulnerabilities and policy issues for congress, *Congressional Research Service*, 2008.

[25] Schultz, E., Continuous monitoring: what it is, why it is needed, and how to use it, *SANS Institute InfoSec Reading Room*, 2011.

[26] Reith, M., Carr, C. & Gunsch, G., An examination of digital forensic models. *International Journal of Digital Evidence*, **1**(3), 2002.

[27] Choudhary, P., A survey on social network analysis for counter-terrorism. *International Journal of Computer Applications*, **112**(9) 2015.

[28] Qiao, M., Sung, A.H. & Liu, Q., Predicting embedding strength in audio steganography. *The 9th IEEE International Conference on Cognitive Informatics*, Beijing, pp. 925–930, 2010.

[29] HilfeTelefon, https://www.hilfetelefon.de/en.html.

[30] Crime Victims Helpline, http://crimevictimshelpline.ie/services-resources/services.

[31] Metropolitan Police, https://secure.met.police.uk/athotline/.

[32] Criminal AFIS, http://pt.nec.com/.

[33] Morpho Video Investigator, http://www.morpho.com/en/public-security/investigate/video-analysis/morpho-video-investigator.

[34] Criminal Justice Information Services (CJIS) compliance, https://www.entrust.com/law-enforcement/.

[35] El-Beltagy, S.R. & Ali, A., Open issues in the sentiment analysis of Arabic social media: a case study. *The 9th International Conference on Innovations and Information Technology*, United Arab Emirates, Mar. 17–19, 2013.

[36] European H2020 TAKEDOWN research project, http://takedownproject.eu/.

[37] Marteinson, P.G. & Michelucci, P.G. (eds), *Applied Semiotics / Sémiotique appliquée*.

[38] Tundis, A. & Mühlhäuser, A., A multi-language approach towards the identification of suspicious users on social networks. *To appear in Proc. of the the 51st International Carnahan Conference on Security Technology (ICCST)*, Madrid, Spain, Oct. 23–26, 2017.