Information & Security: An International Journal

Yavor Dinev, vol.31, 2014, 7-47 http://dx.doi.org/10.11610/isij.3101

LEGAL CONSIDERATIONS OF INTELLIGENCE OPERATIONS IN COUNTERING TRANSNATIONAL ORGANISED CRIME

Yavor DINEV

Abstract: The paper is focused on the application of intelligence operations in countering transnational organised crime (TOC) and reviews the accompanying legal aspects and effects. The purpose of this qualitative paper is to assess the topic from a global viewpoint and establish methodology for examining, evaluating and addressing the execution of intelligence operations, as performed by the global, regional, national, law enforcement or military intelligence entities. The collection of intelligence and the use of liaison may have political or foreign affairs' consequences, hence the importance of considering the existing and applicable legal frameworks or constraints. Some operational approaches cause policy and human rights concerns; however these may be the result of the lack of international or internal cooperation and/or available legal instruments providing for alternatives. The topic is not a time-stamped snapshot but is instead a subject to constant changes in terms of shifting environments and contributing viewpoints for assessing its status, and therefore in need of continual updating.

Keywords: Intelligence, intelligence operations, transnational organised crime, international terrorism, human rights, intelligence oversight.

Introduction

Transnational organised crime transcends national borders, affects societal development and cohesion and fuses the security concerns of local and international civilian and military actors. As such, it has attracted the attention of a number of international and domestic organisations. The leading international organisation focused on countering and preventing transnational organised crime (TOC) on global level is the United Nations Secretariat and its substructure, the United Nations Office on Drugs and Crime (UNODC).

It is closely followed by EUROPOL, the Organisation for Security and Cooperation in Europe (OSCE), the Financial Action Task Force (FATF), the EGMONT Group of Financial Intelligence Units, the Organisation for Economic Co-operation and Development (OECD), the World Bank (WB), the International Monetary Fund (IMF), the Organization of American States (OAS) and INTERPOL in facilitating the coopera-

tion among law enforcement from member countries. Recently, another entity has joined this group. Its name is the *Global Initiative Against Transnational Organized Crime*. Many other international organisations also have statutory or project tasks aimed against TOC; nonetheless the paper will focus solely upon the most important actors.

The major international document guiding the fight against TOC on global level is the *United Nations Convention against Transnational Organized Crime*, having 147 signatories and 179 parties. The convention is effective from 29 September 2003 and includes three protocols, "the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition."[1]

On local, domestic or regional levels the fight against TOC, for instance, and in the case of the US and the EU, is performed by the Federal Bureau of Investigation (FBI) in cooperation with the other members of the United States Intelligence Community and by EUROPOL with the assistance of the EU national law enforcement and intelligence agencies. Domestic or regional actors could engage in global activities individually, through bilateral partnerships or joint agreements with a number of foreign counterparts. Diverse countries have assigned the function of countering TOC to either national law enforcement bodies or intelligence agencies. The threat posed by TOC is not limited to a single country, coming from a single country or aimed at only one sector of the economy. UNODC asserts that the TOC runs through continents and environments where one continent may play a mediatory role for the logistics or contacts required to swiftly move goods, services or technologies to another.[2] According to the FBI, transnational organised crime is rapidly expanding its tentacles to different segments of the economy, including sectors important from a national security standpoint. The perpetrators are diversifying activities by providing services to foreign governments, intelligence agencies and even terrorists.[3]

Transnational criminals participate in smuggling people or goods, misuse the advanced international financial system, its electronic payments and modern services. International organised crime has also expanded its reach in cyberspace, utilising it for illicit operations and committing various frauds and other unlawful operations. The rapid accumulation of immense cash funds allows criminals to corrupt foreign officials and when this is not conceivable for coercion and/or violence.[4]

EUROPOL, referring to Organised Crime Groups (OCGs), notes in its 2013 Serious and Organised Crime Threat Assessment (SOCTA):

> OCGs are increasingly flexible, engaging in multiple forms of criminality. Criminals capitalise on new opportunities in order to generate profit, especially when they are able to use existing infrastructures, personnel and contacts. This is particularly true for groups involved in the transportation and distribution of illicit commodities. OCGs will also expand their enterprises into other supporting or associated activities.[5]

This reference evidently suggests the need for a proactive approach aimed at collecting intelligence against targeted groups and individuals, thus increasing the preventive role of involved government entities instead of relying on *post factum* investigations. The collection of intelligence at international level depends on institutional capabilities and joint or group agreements, while the domestic level presents different set of challenges:

> The FBI routinely organizes task forces with state and local law enforcement officials to pursue joint operations, for instance against organized crime, drug traffickers, or gangs. The local officers work as full partners of the FBI. The rub is that to do so, they need to be cleared to the same level as FBI agents, which is Top Secret (though the clearance process is often expedited).[6]

Law enforcement and intelligence operations have certain and clear distinctions. Law enforcement by definition is investigating and collating evidence with the objective of apprehending perpetrators for processing in a court of law, while intelligence agencies work with information and assets and the classified nature of the collected information does not always allow presenting it in court. Similarly, intelligence agents cannot always appear in court and testify. Some of the challenges faced are purely legal, while others relate to the sharing of classified information with members of the police force or intelligence service of a foreign government. Apart from the official coordination and cooperation, law enforcement agencies from different countries may cooperate or coordinate on an informal level; meanwhile, the same is true for intelligence agencies. According to Bayer, the benefit of informal cooperation is in the joint interest of detaining criminals and in police being equally distanced from major policymakers, foreign affairs officials and intelligence personnel forming the official liaison policies on senior level.[7]

In the field of intelligence the interest in informal cooperation among parties could come from the possibility to exchange information considered valuable and the option to deny the very fact that an exchange has indeed taken place. The need of intelligence operations for countering international organised crime is further emphasised by the links existing among organised crime and terrorism. Transnational crime is often the method used by terrorist groups to accumulate financial resources. Rollins and Wyler claim that terrorists utilise transnational crime for infiltrating countries and environments because it is much easier to corrupt foreign "officials" for "facilitating" the drug trade instead of recruiting an accomplice to a terrorist act.[8]

The purpose of this research is to explore the global possibilities for addressing the use of intelligence operations in countering TOC and figure out the challenges posed by performing similar activities in multiple environments. Exploring the topic would entail taking into consideration the issue of countries' sovereignty, the existing international laws, and the differing and sometimes opposing political systems, because it is apparent that the execution of intelligence operations in countering TOC is a complex matter that brings forward the reasonable question: How do intelligence operations fit within the framework of local and international policy efforts for countering

transnational organised crime undertaken in different jurisdictions? What are the legal consequences of intelligence collection?

According to EUROPOL, the transnational organised crime groups are rapid in implementing private business strategies in operational risk management, sharing, dividing expenses and participating in joint undertakings.[9] The cooperation of transnational criminals is turning into a visible trend which facilitates the swift exchange of arms or other services among crime groups irrespectively of their main location. According to Bergeron, "Crime and security increasingly inhabit a shared space with which the spheres of both defence and policing interact."[10] Comparing the modus operandi of crime groups and government agencies in terms of "gathering, interpreting and applying intelligence to activities and programs" Kenney has asserted:

> While non-state criminal enterprises cannot match the technological sophistication of drug enforcement and intelligence agencies, they possess important advantages over their state adversaries, including the clandestine nature of narcotics tracking, flatter decision making hierarchies, and fewer bureaucratic constraints to action.[11]

The proliferation of transnational organised crime groups, their cooperation and fast accumulation of funds brings to their members access to advanced capabilities, arms and equipment that allows the use of innovative operational intelligence and counterintelligence tactics. Wege asserts that Hizballah is applying advanced counterintelligence employing "electromagnetic spectrum capabilities" and is constantly recruiting professionals from that field.[12] Often Hizballah is looked at as a pure terrorist group; however its structure actively participates in the illegal drug trade and other crime enterprise exchanges.[13] Other terrorist organisations also engage in transnational crime activities as a source for organisational funding. It is no surprise then that terrorist organisations are major players on the TOC scene.

Apart from the global legal framework set-up by the UN and the informal police or intelligence cooperation, the countering of transnational crime and the closely linked terrorism, as well as the undertaking of intelligence operations requires a formalised and streamlined official cooperation in the area of prosecution in different jurisdictions. Complying with this requirement, the US and EUROPOL have agreed in 2001 on joint legal interpretation of terrorism activities, groups, and juridical and operational actions.[14] This agreement facilitates common actions on a juridical level and intelligence operations aimed at terrorism, however it also improves the countering of transnational organised crime groups and, notably, knowing the nexus between terrorism and transnational crime.

The execution of intelligence operations in different countries is a multifaceted matter requiring serious sovereignty and legal considerations from intelligence operators, hence the importance of observing the international legal frameworks and the need of cooperating with other international and domestic actors in the global arena. The planning of these operations would depend on the specifics of the targeted transnational organised crime group. Planners will have to select the most appropriate intelli-

gence method or a fusion of methods for the particular target. They could use Human Intelligence (HUMINT), Image Intelligence (IMINT), Signal Intelligence (SIGINT) or, in some cases known with difficult access, planners may rely on Measurement Intelligence (MASINT), sensors placed on satellites or Unmanned Aerial Vehicles (UAVs).

Some intelligence agencies have units for asymmetric threats while others leave the transnational organised crime to internal security structures. As a result, there could be two different lines in intelligence collection, one of them being the law enforcement path and the second one based on the methods of the respective national intelligence services.

Review of the Literature

It could be argued that there are a plethora of materials—both academic and professional—referring to intelligence operations in countering Transnational Organised Crime (TOC). Nevertheless, it is essential to decide on a framework for addressing the topic of intelligence operations in countering Transnational Organised Crime groups. According to Cockayne, there are three angles for addressing and researching the TOC. It could be approached in terms of inherent activities, viewed as a number of specific and individual entities engaged in criminal activities and by the "effects" it has on multiple environments.[15] The value of the work of Cockayne is in the integral perspective pointing out the environments where TOC flourishes or where the conditions for its surge are ever present. The author notes the increased corrupting power and the effects TOC activities have on surrounding environments. For example, Cockayne incorporates in his working paper findings of Grief suggesting that, "90 percent of the Angolan, 40 to 60 percent of the Russian, 50 percent of the Kenyan, Italian and Peruvian, and 10 to 30 percent of the US economies occur beyond state control."[16] The researcher proposes venues for multilateral responses and drafts sombre hypothetical scenarios. In one of them he argues:

> The worst case scenario is that TOC will slowly corrupt and undermine effective governance at all levels, from the local to the state to the global, corroding global weapons, environmental and health control regimes and fueling armed conflict. In some areas of the globe where state control is weakest, predatory warlords, kingpins and gang-leaders financed by participation in TOC may wrest control of large segments of territory, markets or population away from governments. Powerful states would likely respond by adopting a highly defensive and confrontational strategy, raising significant barriers both within and at their borders to the penetration of OC and terror groups. International relations would be increasingly "criminalized," with powerful states seeking to use all the tools at their disposal—ranging from military force to UN Security Council Resolutions—to control "rogue," "outlaw" or criminalized states, and non-state actors.[17]

Outlining the benefits of Cockayne's work, it should be remarked that while his research is concise and detailed from a multilateral perspective, it lacks focus on the operational side of countering TOC through the instrumentalism of intelligence oper-

ations. There is only one exception and it refers to EUROPOL where the researcher informs that the agency is being used as a medium for directing and coordinating intelligence information among member nations.

Exploring the subject of TOC in UNODC study on Typologies of Transnational Organized Crime Groups, Shaw adds practical details in working out a set of parameters to be used in assessing TOC groups, for instance "Structures, Size, Activities, Trans Border Operations, Identity, Violence, Corruption, Political Influence, Penetration into the Legitimate Economy and Cooperation with other Organized Crime Groups."[18] A general flaw in the studies conducted in the UN system is the absence of references to intelligence or intelligence operations, mainly because of ensuing sensitivities of country members associated with the legal aspects of national sovereignty. Instead, research materials discuss information and information analysis. The UNODC Manuals on Criminal Intelligence for Analysts[19] and Managers,[20] issued in 2011, as well as the paper on *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* from 2009,[21] are illustrations of this point and demonstrate that there could still be occasions when the general practice is waived in order to incorporate the latest trends in intelligence-led policing for preventive action.

Having an insight on a TOC group facilitates the targeting process to be developed by the planners of intelligence operations. The Research and Evaluation Branch of the Royal Canadian Mounted Police (RCMP) has produced a paper on "The Changing Structure of Organized Crime Groups."[22] The study posits that nowadays the world of organised crime groups is much more intricate and flexible than previously considered. It could be characterised as having home bases and forward stations in areas of operations which provide fast income opportunities. The work of the RCMP draws from the 2002 UNODC "Pilot Survey of forty selected organized criminal groups in sixteen countries," stating for example:

> The major Colombian cartels provide a good example of complex network type structures. Their structure is compartmentalized, and mimics a large, multinational corporation – with the home-based president and vice-presidents making decisions, monitoring and managing the acquisition, production, transportation, sales and finance for the drug-trafficking "business," and the overseas cells handling the import, storage and delivery of the product, as well as money laundering.[23]

In 2010, the office of Research and National Coordination at the Organized Crime Division of the Law Enforcement and Policy Branch of the Public Safety Canada issued a follow up report on "The Factors That Shape Organized Crime."[24] While the RCMP paper viewed organised crime groups from the viewpoint of constantly evolving structures; the work of Morselli, Gabor and Kiedrowski focused on parameters forming the organised crime. The former paper is interesting from an intelligence analyst's perspective in figuring out the future trends of TOC groups, while the latter is particularly suitable for utilisation in the planning process and during the conduct of intelligence operations. And even though this is not mentioned in the work, it is hinted in the context:

> …this framework suggests that the most obvious forms of manipulation that are at law-enforcement's disposal are the basic decisions of when to control and to what degree should control take place. Such decision-making is clearly not new for law-enforcement officials. What must be retained here is the outcome of that decision – its effect on organized crime. Law-enforcement officials must be aware of how their actions will shape the structure of organized crime. Indeed, they are in a position to foresee such outcomes.[25]

The instrumentalism of intelligence in countering transnational organised crime includes the use of Human Intelligence (HUMINT), Signal Intelligence (SIGINT), Image Intelligence (IMINT) and Measurement Intelligence (MASINT) under the form of remote drug and substance sensors or scanning sensors for geographical environments, facilitating the establishment of potential tactical approaches to targets. The use of HUMINT is perhaps the most problematic in the sense that assets may not be always individuals of proper ethical and moral standings, particularly in the field of TOC. In an article on multinational intelligence cooperation, Lansford notes the difficulties in that regard faced by the US Intelligence Community:

> U.S. HUMINT capabilities were constrained by a series of restrictions put in place beginning in the 1970s. These limitations were expanded in 1995 by new prohibitions on the ability of the CIA and other intelligence agencies to recruit or work with people who may have committed human rights violations. Former CIA Director James Woolsey criticized the restrictions in the following manner: "It's like telling the FBI they can recruit informants inside the mafia, but they can't recruit crooks."[26]

The work of Lansford, though intriguing, is similar to other papers treating the issue of intelligence and intelligence cooperation from the perspective of intelligence cooperation *per se*, among allies mainly, and circles around counterterrorism efforts. Many researches treat the effort of countering transnational organised crime as secondary to terrorism, and an analogous approach misses the links existing among terrorism and TOC. There is constant fluidity of activities and members between terrorists and organised crime groups, intersecting in the ways they finance operations or excavate profits from illegal undertakings.

For example, Nemeth describes the relationship between TOC and terrorism by pointing out the misuse of art and artefacts in the international art market. It is a known fact that profits from the sale of artefacts may be enormous, and not only that, but art could be used as a form of payment for arms or other illegal deals. Overpaying for art during auctions is not prohibited by law and instead provides for entirely legal transfer of funds among two concerned criminal parties:

> A link between antiquities trafficking and funding of terrorists creates a paradox for those collecting nations that also combat terrorism. If terrorist groups do facilitate the looting of cultural artifacts, collectors who purchase such artifacts not only participate in the illicit trade of cultural property and the destruction of cultural heritage but also risk the implication of supporting terrorists.[27]

Summarising Nemeth's angle, terrorist leaders use the lack of income opportunities in the villages close to their respective training bases to motivate local population to collect and search for valuable antiques. These artefacts are then exported and auctioned abroad through money laundering schemes where the TOC arranges for export facilitation, auctioning, bank account creation and wire transfers to the respective terrorist group.[28]

A recent practical example for the links among transnational organised crime, terrorism and state actors, as well as their co-operation, is rendered by Kershner in an article published in New York Times. The author informs that Israeli commandoes have intercepted a ship in the Red Sea. Apparently, the ship has participated in a smuggling operation intended to deliver an Iranian consignment of Syrian made rockets to the Hamas movement in Gaza strip. The Israeli authorities have established that the range of these missiles has been much longer than the one so far used by Hamas. In a classic smuggling operation typical for transnational organised crime, the rockets were initially flown from Damascus to Teheran, moved to an Iranian port, loaded on to a ship supposed to take cement cargo in Iraq and headed for a Sudanese port known among arm traffickers as a "transit point" for arms heading for the Palestinian territories.[29]

The participation of state actors in the TOC or its use for achieving ethnic or national political goals is of particular concern for policymakers. Similar interaction not only provides a cloud of security or invincibility for illicit transnational networks but also increases and extends their capacity and ability to perform complex operations unhindered, and in diverse jurisdictions. Of no less importance in terms of increased threat is the TOC establishing personal "business" contacts with foreign officials, thus increasing the future spectrum of areas and scopes of their illegal operations.

Collecting intelligence on transnational organised crime groups and members could involve police, military and national intelligence structures. Nonetheless, these three entities have different modus operandi and the collection and subsequent analysis requires a great deal of joint work and sharing. As an illustration, Cordner and Scarborough (2010) have drafted a table outlining the responsibilities of the national security structures in the US:[30]

The work of Cordner & Scarborough provides an insight into the US approaches for cooperation among police, military and national intelligence services. Another national perspective, the Brazilian for example, is outlined by Mingardi. The researcher discusses the use of intelligence work in controlling organised crime and makes an effort to differentiate among investigative and intelligence work. Mingardi argues that the former is relying on collection of hard facts and evidences while the latter may have as a basis rumours labelled as information, however still be used for police action. The author notes that the proceeds of investigations could be presented in the court of law, while the product of intelligence work is used for an analysis of trends and the building of policies:

Table 1: Division of Responsibilities of National Security Structures in US.

	Domestic Crime	Transnational Crime	Terrorism
Local Police	Primary responsibility for prevention, response, and investigation	Growing problem associated with globalisation and Internet; limited by resources and jurisdiction	Eyes and ears throughout the country; closest to the public (human intelligence); first responders and infrastructure protection
State Police	Varies by state; Some primary and some secondary responsibilities; Important support roles- crime labs, criminal records systems, and so forth	Growing problem associated with globalisation and Internet; Limited by resources and jurisdiction	Eyes and ears, information collection and analysis first responders and infrastructure protection
Federal Law Enforcement	Investigation of federal crimes, protection of federal property; Important support roles: crime labs, criminal records, special expertise	Long-standing focus with regard to drugs, smuggling, customs, border control, and so forth; becoming even more salient due to globalisation and Internet	Primary responsibility for investigation and operations within the United States; information collection and analysis; liaison to national intelligence agencies
Federal and State Homeland Security	Little or no federal homeland security role; State fusion centres adopting all crimes approach	Important focus for state fusion centres; some federal focus due to the nexus between crime and terrorism	Intelligence analysis and information sharing
National Intelligence	Little or no role; restricted by law	Little or no role except when connected with terrorism	Investigation and operations outside the United States; Intelligence analysis and information sharing
Military	Little or no role except on military bases or involving military personnel; restricted by law	Support role over the past 20 years with regard to drug smuggling; otherwise limited to military bases and military personnel	Military operations outside the United States; Homeland defence; Military operations within the United States through NORTHCOM

> In other words, the work of Intelligence is much more opinionative than that traditionally conducted by the judicial police. There are other basic differences between the work of Criminal Intelligence and Criminal Investigation, which distance the two activities even more and often cause misunderstandings on each side. In an investigation, the detective or prosecutor works with individual cases and needs proofs. The information they seek has to have immediate usefulness, because it is seen as part of an ongoing investigation. The results of Intelligences, however, are of a longer term, and in most cases, do not serve as proofs. Therefore, the greater separation between the operational and the Intelligence field the better.[31]

Apart from the police and intelligence services, timely criminal intelligence is also important for the prosecutors in the performance of their duties. The prosecution services usually rely on receiving analytical products from other agencies. The investigations of organised crime groups operating in multiple countries may naturally involve the use of modern surveillance technics, HUMINT assets or undercover officers. The dangers related to infiltrating and maintaining status and reputation in transnational organised crime groups, as well as the ethical and moral considerations, could cause prevalence of SIGINT methods, including interception of communication traffic going through satellites. Conversely Dandurand asserts that no international investigation can be launched without the establishment of a proper international cooperation among the concerned entities.[32] The antithesis is possible in cases of covert or clandestine operations, sometimes through the utilisation of paramilitary units against highly armed and tactically sophisticated organised crime or terrorist groups. Nonetheless, analogous actions are carrying legal and political risks that may ensue in diplomatic confrontation. According to the US Department of Defense (DOD):

> Defense officials have asserted that none of DOD's current counterterrorism intelligence activities constitute covert action as defined under the law, and therefore, do not require a presidential finding and the notification of the intelligence committees. Rather, they contend that DOD conducts only "clandestine activities." Although the term is not defined by statute, these officials characterise such activities as constituting actions that are conducted in secret but which constitute "passive" intelligence information gathering. By comparison, covert action, they contend, is "active," in that its aim is to elicit change in the political, economic, military, or diplomatic behavior of a target.[33]

The threat of the TOC is recognised on a most senior level of democratic governments around the world. Back in 1997, when Tony Blair's government assumed power in UK, it adopted an "interventionist" policy in the field of foreign affairs and recognised that intelligence services should play a bigger role in formulating approaches including the fight with organised crime, "Blair was also keen to see the intelligence services in the frontline of the war against organised crime and held a Downing Street summit on the subject in 1999."[34] The Détente, the shrinking budgets and the 9/11 have all clearly pointed out the direction of facilitated intelligence cooperation and liaison among countries. Intelligence sharing and joint operations may

take place between current allies, former allies or on a case by case basis depending on the interests and the commonly accepted rules for working with the information received by liaison counterparts. For instance, the EU and the US have had different understanding of terrorism before 9/11 and the political perspective prevented real intelligence cooperation in the field of antiterrorism and counterterrorism. Following 9/11, the atmosphere changed almost overnight:

> But even in the initial aftermath of 9/11, the Director of EUROPOL, Juergen Storbeck, warned against rushing to blame the Saudi-born militant Osama bin Laden for masterminding the attacks on New York and Washington, stating: "It's possible that he was informed about the operation, it's even possible that he influenced it, but he's probably not the man who steered every action or controlled the detailed plan." By the next morning, this view had changed to "Over the next week, we will travel to the United States with a delegation from the Belgian presidency of the European Union to begin talks on a cooperation accord."[35]

The threat posed by the TOC is monitored on national and international level by the intelligence agencies of nation states. The monitoring involves the undertaking of intelligence operations of various types and methods. The annual reports of national intelligence agencies therefore contain non-confidential, however revealing consignment of information, about focus of activities and main threats. As an illustration, Bundesamt für Verfassungsschutz (BfV)—the German Domestic Intelligence Service—in a 2012 report notes the various types of extremism existing in Germany but from the content it is obvious that the service is not considering the TOC as a threat to the Constitution.[36] There are references to left, right-wing and radical extremism; yet no mentioning that all these groups could rely on criminal activities for funding, procuring weapons, planning of operations and cyber activities, hacking included. The diverged BfV focus may have its basis in the division of responsibilities within the national security architecture of Germany. For instance, Bundeskriminalamtes (BKA)—the German Federal Criminal Police office—is the entity that has functions in countering international organised crime. In 2011, BKA issued a quantitatively oriented Organised Crime National Situation Report, full with statistical data, allowing for planning of intelligence operations aimed at targeting organised crime groups. In other words, if the German authorities decide to target the Russian organised crime groups they should focus on cybercrime and initiate cyber intelligence, and nonetheless utilise also HUMINT. In contrast, German nationals' and other ethnically based organised crime groups are having the drug trafficking and smuggling as their main choice of illegal activity.[37]

Similarly to their German counterparts, the Czech Republic counterintelligence service, the Security Information Service (Bezpečnostní Informační Služba, BIS) also pay attention to left, right wing extremism and radical Islam. On the other hand, their responsibilities include the organised crime. The BIS 2012 report informs that apart

from the domestic organised crime groups, active on the territory of the Czech Republic are groups with Armenian, Georgian, Vietnamese and Balkan origins. Of particular interest for this paper is the observation on BIS cooperation with the Federal Security Service of the Russian Federation (Федеральная Служба Безопасности Российской Федерации, ФСБ/ Federalnaya sluzhba bezopasnosti Rossiyskoy Federatsii, FSB) in the field of regular police work and counter terrorism. The Czech counterintelligence service has established that there were occasions when an intelligence officer of the FSB has used its participation in the fight against terrorism or in provision of police assistance in countering organised crime as a cover for real duties. Additionally, the BIS 2012 report notes the attention of the Czech counterintelligence to preventing the trafficking and sale of weapons of mass destruction, prohibited technologies and the increasing occurrence of cybercrime activities.[38]

Poland's counterintelligence, the Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego, ABW) likewise announces achievements in the fight with international organised crime. The 2009 ABW annual report identifies specific cooperation among illicit networks, namely the Polish crime contingent has trained organised crime counterparts in Sweden, UK, Ireland and Ukraine on the production of amphetamines. This move benefited the launching of amphetamine laboratories in these countries, consequently avoiding the need of engaging in risky cross border smuggling operations. ABW reports that a joint operation with the US Drug Enforcement Agency (DEA) and the Columbian Police has led to the successful interception of 1154 kilograms of cocaine trafficked from South America to Europe by an international organised crime group operated by Dutch, Austrian, Columbian and Venezuelan citizens.[39]

The Danish Security and Intelligence Service, Politiets Efterretningstjenestes (PET) provides an annual 2008-2010 report that is particularly detailed, instructive and inquisitive reading. Among the other duties, PET has responsibility in the area of countering the serious organised crime:

> PET deals with serious organised crime characterised by its international, cross-border and professional nature. This form of crime is committed by use of violence, threats and weapons in hard-to-infiltrate environments where the perpetrators are extremely security-conscious.[40]

The report notes interesting cases in PET operational experience. For instance, the investigation of sizeable weapons cache robbery from a military base involved PET because of the aggressiveness of the theft and the large number of stolen weapons. The conclusion of the investigation has led to the detainment of Danish military personnel on the territory of Denmark as well as on the territory of Kosovo. In another case, PET blocked the operations of international cannabis network transporting cannabis from Spain to Denmark with Mercedes cars driven by East Europeans. A Spe-

cial Operations unit of PET has the authority to use the assistance of civilians recruited as agents in the capacity of sources or informers for particular task/s, as well as to infiltrate serious crime groups through the use of undercover career officers. In terrorist cases the infiltration could be performed without receiving court order in advance. The work of planted Danish undercover agents has facilitated a DEA investigation. In 2009 the HUMINT of PET has infiltrated a cocaine smuggling network, that was moving immense loads from South America to Africa and subsequently to Europe among the other destinations. This case is of particular interest because it displayed the relations existing among international criminals, insurgent movements and terrorists, arms and cocaine trafficking on global level. The findings have led to the subsequent arrest of a Russian arm trafficker in Thailand trying to supply Fuerzas Armadas Revolucionarias de Colombia (FARC) with arms and a mastermind of cocaine ring in Romania. Both individuals are currently in the US awaiting sentence. The Columbian FARC appears twice in the report of PET – the second time in regard to the interception of a Swedish national trying to make the barter of weapons for cocaine. PET is also having an in-house Special Intervention Group which among the other tasks is closely involved in "fighting terrorism and serious organised crime by providing sound options for performing different police assignments where the standard police training and equipment is not adequate."

One of the major crime activities and bloodline of transnational organised crime groups is the laundering of illegal proceeds. On global level it is the EGMONT Group of Financial Intelligence Units that is countering the money laundry through policies and operational directives, while on national levels we have the respective financial intelligence units.[41] The 2012 Anti-Money Laundering Report of the Swiss Federal Police offers an example of a national specific. Under the Swiss Law, the Federal Supreme Court after examining the details of an investigation launched by the Office of the Attorney General may rule a regime as a 'criminal organisation.' Most recent cases relate to declaring the whole regime of Hosni Mubarak as a criminal organisation, and likewise for the regime of Gaddafi.[42]

As seen from the information found in the reports of the national intelligence agencies, the collection of intelligence on transnational organised crime groups necessitates international co-operation. Compounding on the role of international cooperation, the work of Wippl presents the idea of creating an Intelligence Interpol for sharing international intelligence. The author asserts that foreign intelligence services have more reasons to cooperate in the operational field than their domestic counterparts.[43] Wippl clarifies the idea for "InterIntel":

> Such multilateral intelligence exchange must be a service organisation for the participants. It must answer questions for the participants about transnational organisations, not limited to terrorism, but including proliferation and organised crime, as well as other issues.[44]

The annual reports of different national intelligence agencies, whenever public, provide factual insight on the specialisation of tasks related to the countering of international organised crime, the corresponding intelligence operations and the capacities of involved personnel. Besides, they inform on the specific types of international organised crime groups and illegal activities existing in particular countries or regions.

In the case of Europe, all criminal intelligence accumulated on national EU member countries level goes to EUROPOL for further recording and analysis from Europe-wide perspective. Indeed, EUROPOL is also engaged in international cooperation. According to Segell, the current cooperation among EUROPOL and the US is based on an agreement from December 2001 and includes European Arrest Warrant. Meanwhile, EUROPOL has already evolved as the leading criminal intelligence agency of the EU, assisting national authorities with information, analysis, planning, information and communication technology, and training capabilities. EUROPOL's intelligence databases facilitate national and international effort; yet, they are also reasons for concern among the human rights activists. In fact, a name of an individual can get inside only because a national authority may "believe" that a person is involved in the crime activities outlined under the tasks and duties of EUROPOL. For example:

> Police control has been extended to a level which has rightly been characterised as "proactive," since it is provided that data to be inputted in the EUROPOL information system do not only pertain to those suspected of having committed a given crime, but also to those suspected of committing a crime in the future, or even those who merely get in touch with such suspects, i.e. persons who are aloof of any concrete criminal act.[45]

Kastanidou understands the effects of organised crime groups on societies and international relations. Nonetheless, she is making the point that increased surveillance capabilities would affect more the life of regular EU citizens than the activities of affluent criminals able to afford high tech secure communication equipment and capabilities for countering interception by law enforcement agencies. The same author believes that similar development will lead to digression on the path of the civil liberties earned by the modern societies. In this regard, it is fair to note that achieving balance among the need to counter national security threats while maintaining personal liberties is not a task with guaranteed outcome. As challenging as it may be, the task is nothing more or less than a path to walk on and discover.

Methodology and Research Strategy

The use of intelligence operations in countering transnational organised crime is a complex matter that cannot be quantified in terms of numbers for pragmatic reasons, some of them related to classified information. The intelligence operations in countering TOC could be regarded as a subdivision of the local or foreign intelligence operations of the respective intelligence communities or law enforcement entities. Bearing

in mind their sensitivity, unintended effects and consequences, the intelligence operations are an area of special concern for policymakers.

While intelligence communities may release some confidential operational information after the passage of certain number of years, depending upon the national legislation, it is also possible to withhold the release of files to the public. One reason for adjourning declassification may lay with the fact that particular content could create threats to the country of concern or to the intelligence agents involved in the initial collection process. Another reason is linked to the Mosaic Theory making the point that pieces of released non-confidential information may lead to conclusions that will threaten national security, when reviewed or examined by adversaries: "Thousands of bits and pieces of seemingly innocuous information can be analysed and fitted into place to reveal with startling clarity how the unseen whole must operate."[46] This inherent complexity and constant sensitivity of the intelligence operations in general requires that the study author approaches the structuring of the report through the lenses of qualitative methodology, where the word "qualitative" is defined as in the following way:

> The word qualitative implies an emphasis on the qualities of entities and on processes and meanings that are not experimentally examined or measured (if measured at all) in terms of quantity, amount, intensity, or frequency. Qualitative researchers stress the socially constructed nature of reality.[47]

Contributing to the selection of the research methodology is the fact that intelligence is adjacent to social science and draws heavily upon cognitive science. Decisions taken by adversaries or transnational organised crime groups' heads are individual and depend upon their social constructs and internal psyches. Similarly, in the analysis of foreign affairs or transnational organised crime groups, the constant is always the human element and it is the human factor that propagates its system of values, political, personal views and interests or demonstrates propensity for adherence to criminal or terrorist behaviour. In both cases there is a reference to collective forms of human behaviour, hence the visible connection with social psychology and the collective psyche or, said otherwise, the "collective unconscious."[48]

The research underlying this paper obtained its data through analysing available academic and professional literature in the field of Intelligence and Intelligence Operations. In its pursuit, the author applied the Grounded Theory of Glaser and Strauss to facilitate the study of the phenomenon of intelligence through review of existing public materials.[49] As a structure, the study moved from global to local, general to specific issues, noting major transnational crimes as well as specifying the existing international legal framework for countering transnational organised crime groups.

Hence, this paper will outline the corresponding types of intelligence operations and summarise the approaches of law enforcement and mainstream intelligence organisa-

tions on formal and informal levels. The side effects accompanying the execution of intelligence operations would impose the question, "What are the legal implications of conducting intelligence operations against transnational organised crime groups?" and consequently the research will examine the legal effects of intelligence operations.

The qualitative methodology selected for this paper implies inductive reasoning and the inductive reasoning demands a stated hypothesis. The hypothesis states that intelligence operations in countering transnational crime epitomise an area of general interest where countries from different regions of the world may have substantial cooperation, as opposed to other areas of intelligence characterised by political and economic competition and rivalry. The research of the available academic and professional sources will stipulate the direction of the emerging theory. The exploration of the literature will entail "memoing" as an analytical strategy.[50] This particular approach requires the noting down of all ideas that appear or change during the research process and posits that the natural evolution of the paper brings greater focus. While quantitative methodologies may call for evaluating, analysing and observing specific and required fixed numbers of data, information or events before reaching statistically supported conclusions, the grounded theory and qualitative research methods are not concerned with a specific number of obligatory observations. On the contrary, the research performed under grounded theory assumptions exemplifies a constantly evolving process with time or process length reliant upon the researcher's decision, and whether the collected and explored sources are sufficient for building an initial theory concerning a phenomenon.

The two independent variables of the paper are the constantly evolving international legal systems and intelligence cooperation, while the two dependent variables will be improved prosecution and increase in international joint intelligence operations. Referring to the first independent variable, an argument of Jamieson in an article about the cooperation of organised crime groups provides for eventual direction in the development of the modern legal system:

> The only way to meet the challenge of organized crime in the next century is to reinforce international legal instruments that unite measures of prevention, that is, regulation through civil law, with those of repression, that is, application of criminal law. In isolation, neither prevention nor repression will be sufficiently effective. Virtually all the necessary legislative tools have been elaborated and exist on paper in the form of draft or signed conventions or agreements, but they require to be ratified by all governments and applied with rigor and political will. To place the accent on international instruments inevitably means a loss of sovereignty. But it could be suggested, firstly, that sovereignty has already been lost, and secondly, that it may be a necessary sacrifice if we wish to save our democracies from the stranglehold of organised crime.[51]

As for the second independent variable, following the 9/11 terrorist attacks there has been "dramatic improvement in intelligence collection and sharing" and "in bilateral cooperation with other nations – those we considered friendly before 9/11, and some we considered less friendly."[52] The limitations in performing the research may come from the limited access to intelligence literature. Kent asserts:

> The first of these is probably the matter of security. One can expect the question: "Do you want to put all the secrets of the profession in writing and bind them up in one great book so that your enemy's success with a single target will at once put him abreast of you?" The answer comes in two parts. In the first place, many of the most important contributions to this literature need not be classified at all. They could be run in the daily press and our enemies would get no more good from them than from the usual run of articles published in our professional journals.[53]

A second limitation may arise from using prevalently Anglo-Saxon literature, examining issues through perhaps fixed lenses. Nonetheless, it would be fair to note that profound and academic, non-confidential level discussions of intelligence takes place mainly in Anglo-Saxon universities and educational institutions, thus this may be the only opportunity for researchers to touch upon the subject and explore it in detail. Countries may have restrictions on teaching the subject to the public at academic level, or it may be taught only to career intelligence professionals in government intelligence colleges. The first non-Anglo-Saxon centre for studying the phenomenon of intelligence in the German speaking world is the Austrian Centre for Intelligence, Propaganda and Security Studies (ACIPSS). It is issuing a Journal for Intelligence Propaganda and Security Studies (JIPSS), yet a large number of its articles are in German language, thus limiting the ability of English speaking researchers to assess all materials. Another European centre for intelligence studies is located at the University of Calabria in Italy. The centre has a signed cooperation memorandum with the Mediterranean Council for Intelligence Studies at the Research Institute for European and American Studies.[54]

A third limitation would come from the immense number of available sources and the constrained timeframe for conducting the research, consequently affecting the depth of the conclusions and their reliability.

The fourth and final limitation would originate from the fact that all studies represent a time-stamped snapshot of a particular phenomenon. Theories constantly change, besides the parameters of our existence, awareness and understanding is changing as well, and however prosaic it may sound, "nothing in life is carved on stone" *in mundus sensibilis*.

* * *

> There are not more than five musical notes, yet the combinations of these five give rise to more melodies than can ever be heard. There are not more than five primary colors (blue, yellow, red, white, and black), yet in combination they produce more hues than can ever be seen. ... In battle, there are not more than two methods of attack – the direct and the indirect; yet these two in combination give rise to an endless series of maneuvers.
>
> —Sun Tzu, The Art of War [55]

Findings and analysis

The findings and analysis describe selected assessments on intelligence operations conducted on domestic and international levels. In both cases they refer to targeting transnational organised crime groups. Furthermore, the topic of transnational organised crime (TOC) is addressed in the sources from the policy and operational angles. Most of the available sources assign to United Nations and its Convention against Transnational Organized Crime and the Protocols on the Trafficking in Persons and the Smuggling of Migrants by Land, Air and Sea a major policy role in addressing the TOC from global perspective. Other organisations working on impacting the policy level in countering TOC include, but are not limited to the Organisation for Economic Cooperation and Development (OECD), the Organization of American States (OAS), the Organisation for Security and Cooperation in Europe (OSCE), EUROJUST, the Association of South East Asian Nations (ASEAN) and the Global Initiative Against Transnational Crime. The perspective applied by these organisations in viewing TOC is varying and subject to regionalisation or field of expertise.

The operational angle involves national intelligence communities, regional or global organisations like for instance, EUROPOL, INTERPOL, Federal Bureau of Investigations (FBI), Canadian Security and Intelligence Service (CSIS), Australian Secret Intelligence Service (ASIS), World Customs Organization (WCO), International Tracking Instrument (ITI), etc. These organisations have as task the countering of transnational organised crime on global, regional level or addressing only specific forms of its appearance. Some regions and regional players or countries assume global role or tasks, whereas others' efforts remain constrained and internally motivated. The operational level also requires policies but these are needed for back up and guidance in regard to field actions. For example, the US have a National Strategy to Combat Transnational Organized Crime. From the perspective of this paper, two of its total of five key policy objectives represents an interest for observation:

> 4. Defeat transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.
>
> 5. Build international consensus, multilateral cooperation, and public-private partnerships to defeat transnational organised crime.[56]

EU on the other hand is looking for synergies in joint action. The UN Convention against Transnational Organized Crime is implemented in the EU laws and EU is following strictly the advice of Financial Action Task Force (FATF) on anti-money laundering. The major areas where the transnational organised crime groups engage in illegal activities are arms, drugs and human trafficking, cybercrime, environmental crime, financial crime and money laundering, piracy and infiltration of governmental and development sectors in fragile states and economies. It is important to note that criminal activities could be a part of converging threat vectors similar to the transnational crime-terrorism nexus in numerous combinations. As an illustration, Admiral Stavridis notes:

> These transnational organisations are a large part of the hybrid threat that forms the nexus of illicit drug trafficking—including routes, profits, and corruptive influences—and terrorism, both home grown as well as imported Islamic terrorism. With the latest wave of globalisation allowing for even more movement of people, goods, and information, these actors have spread their tentacles wider and deeper, breaking new ground.[57]

A substantial reason for the existence of transnational organised crime groups lays in the arbitrage possibilities created by the globalisation where a good, commodity, service or an activity, outlawed in a jurisdiction, presents an opportunity for local or foreign actors to exploit and amass profits in short time by assuming the corresponding risks and legal consequences. Hence the appearance of the so called fixers or undertakings focused on facilitating criminal activities. Outlawing a good, commodity, service or an activity leads to reducing its availability and an increase in prices. The countering of TOC on global level implies the need of acquiring proper information; *ergo*, it indicates the need of collection, analysis and consequently designing intelligence operations for targeting transnational organised groups, their members, activities, investments or funds:

> A shift in U.S. intelligence collection priorities since the September 11, 2001 attacks left significant gaps in TOC-related intelligence. Meanwhile, the TOC threat has worsened and grown in complexity over the past 15 years. The fluid nature of TOC networks, which includes the use of criminal facilitators, makes targeting TOC increasingly difficult.[58]

While national, state or federal agencies may have intelligence capacities in collection, analysis and targeting, the same may not be true for provincial or police authorities. The authorities that are constantly in the field or the street are also the government structures that have the opportunity to observe, monitor or be in direct touch with organised crime group tendencies and appearances on ground level. Exposing these authorities to intelligence training or building their intelligence capacity is contributing to an increase in the number of detained organised crime group members, to

stronger analytical aptitude and ability to plan or participate in intelligence operations initiated on higher levels:

> Intelligence operations have been reviewed, studied, and slowly but steadily transformed. Most efforts have focused on reorganising intelligence infrastructures at the federal level; however, corresponding efforts have been made to enhance state and local law enforcement intelligence operations. Such enhancements make it possible for state and local law enforcement agencies to play a role in homeland security. Perhaps more important, improvements to intelligence operations help local law enforcement respond to "traditional" crimes more effectively.[59]

According to Kenney, the intelligence consumed for countering the drug trafficking is strategic, operational and tactical. The strategic intelligence serves for assessing global trends and facilitates policymakers and organisations in designing policies. It is not used for investigation purposes because it has wider focus. Operational intelligence relates to existing short, long term operations or investigations in the field with time length of few months. Some entities divide operational intelligence on strategic and tactical therefore foreseeing the possibility of intelligence operations continuing much longer than few months. Tactical intelligence instead is used for capturing organised crime groups or individual members or in seizing or targeting their criminal assets. The tools of strategic, operational and tactical intelligence are also applicable for countering the other types of TOC. For example, Abadinsky notes the existence of strategic and tactical intelligence but misses the operational intelligence in its work. The author is however dividing operational intelligence content among strategic and tactical intelligence.[60] Another detail comes from the ways in which intelligence for countering transnational organised crime is viewed by authors. For instance, Abadinsky sees intelligence as an investigation tool while the Brazilian researcher Mingardi is in fact openly advocating for substantial distancing of the intelligence process from investigations.[61] According to Mingardi, collected intelligence may be based on unsubstantiated information or, otherwise said, rumours. Similar difference of opinions may be explained with eventual lack of understanding of the concept of intelligence led policing in law enforcement as well as with possible weaknesses of the Brazilian intelligence system.

Different types of TOC may have particular specifics, that differentiate them in the modes of collecting intelligence. Most notable in this respect are the sectors of cybercrime and terrorism financing, high level corruption and money laundering, where the detaining individuals or seizing assets may require serious and long term intellectual efforts. For example, the countering of cybercrime, apart from possible HUMINT and IMINT, may call for specific intelligence operations in the cyber realm not limited to a static SIGINT. EU has recently realised the increased importance of protecting member countries' governments and private cyber infrastructure and has called for

aggressive cyber intelligence, cyber counterintelligence and targeting of not only government but also private, non-state targets.[62]

FATF and OECD have strategic policy role on global level in the performance of their statutory activities. The specifics in the work of FATF in countering the financing of transnational organised crimes in its subpart related to terrorism, money laundering and high level corruption involves intelligence collection for producing strategic intelligence reporting and policy papers. The intelligence collection could be performed locally and shared through FATF or other international structures, or may be a result of corporate undertaking related to internal investigations in regard to financial instruments provided to member countries or public, private entities by the IMF, the World Bank and/or other similar institutions.

An example in case is the financing of the proliferation of WMD. A WMD could be produced by mixing dual-use substances and, consequently, the ability to link particular financial transaction to their production is in many cases a difficult task. As FATF has established, intelligence services may be the necessary to provide the link among financiers, participating financial institutions, transnational criminal enterprises or individuals with destination countries, groups, recipients and clients:

> In many jurisdictions, competent authorities, including export control and customs agencies, may also use intelligence information about possible suppliers or end-users of goods with a potential dual use in a WMD program when deciding whether to grant an export license or to let goods pass the border. Some jurisdictions have developed profiles of suspicious suppliers on the basis of infringements of export control provisions or end users based on intelligence which customs agencies use to trigger catch-all provisions. … Intelligence services therefore play an essential role in identifying individuals and entities who may be involved in or supporting the financing of proliferation of WMD.[63]

FATF as an international structure formed by G-7 also produces guiding papers aimed to support and facilitate the operational part of financial investigations. Depending on countries and national laws the operational functions may be assigned to law enforcement or national intelligence agencies. Hence, the investigative techniques developed by FATF serve two purposes and are also telling of the intelligence operations in countering other transnational organised crimes. FATF recommends the following operational approaches in investigation and intelligence work.

Physical surveillance

The aim of physical surveillance is to establish the contact points and personal networks of persons of interest, evaluate their routines, build their profiles and check used premises for explicit documents, cash or substance availabilities.

Checking garbage

At times suspects may discard or throw shredded documents which, if found or re-composed, could lead to important evidence that could be used in the court of law.

Use of search warrants or similar legal instruments

These are obtained if the physical surveillance cannot provide results and in cases of restricted, highly guarded or electronically protected entry. Used on occasions when there is information, intelligence or awareness that particular part of the investigation or development may force the suspect (person, group or entity) to destroy or move evidences, substances, goods or objects. FATF points out that official searches and evidence gathering should be accompanied by custom built procedures for storing and safekeeping of these evidences and by involving digital forensic examiners for digital data and IT components.

Inviting suspects or person of interest for unofficial meeting

The focus will be on voluntary solicitation and collection of relevant information. The voluntary nature could be changed to handing an officially binding request in compliance with local laws. Analogous meetings should be held only if they do not affect the work of the corresponding investigative or intelligence unit on the opened case.

"Controlled delivery"

This is a technique presenting opportunity for disrupting the activities of transnational organised crime groups when properly planned, coordinated and executed in compliance with operational security principles and in line with the security clearance levels of local or foreign officials, as well as in coordination with other relevant and involved law enforcement or government bodies. Its application allows for positively identifying participants and new groups or individuals in ongoing investigation. The identification of used assets and wider network facilitates the establishment of initially invisible connections and links these assets to particular participants, thus securing evidence for court proceedings.

SIGINT

The purpose of SIGINT is to intercept fixed line, digital and satellite communications, internet traffic or install listening devices or bugs for localising physical presence of objects or individuals. It is important that interception is performed in line with local laws so that it cannot be attacked in a court of law. The use of SIGINT by law enforcement or national intelligence agencies may have as a goal simply the collection of information on a specific target without considering or planning for any legal or court proceedings.

HUMINT

HUMINT is used for infiltration of transnational organised crime networks by law enforcement or intelligence officers or through the recruitment of agents among the criminals, if the respective laws or internal regulations do not object similar approaches.

Locating proceeds of criminal activities and connecting these to individuals, groups, networks or specific activities

This method is focused on collecting evidences for building cases in courts of law and drafting schemes of organised crime networks.[64]

While the above investigative techniques could be applied by law enforcement and intelligence units toward all TOCs, it should be noted that the "controlled delivery" is not always an option in investigating terrorism cases. It could be allowed for the delivery of materials or resources but not allowed in observing a real terrorist act, unless of course the delivered explosives are fake and can never explode, while can still prove intent. The importance of communication interception as a SIGINT method is noticed by many researchers. For example the Australian researcher Bell advocates for greater use of interception technologies; however duly notes the legal constraints in regard to using similar technologies by the police force as opposed to intelligence agencies. One reason for this distinction comes from the existing legislation and the need of warrants when Australian citizens in Australia are being investigated.[65]

Bell notes that the transnational organised crime cannot function without communication and coordination of actions and these activities take place through the use of mobile devices, satellites and internet. The TOC is fast in applying detection prevention tactics by purchasing batches of chip pre-paid "burner phones," applying commercially available encryption technology, stenography and anonymous web-mails.[66]

Of particular importance in the use of communication interception is the difference among live and stored communications since this indicates the operational approaches for preparing interception on particular device or on accessing data stored on the servers of a particular service provider. The former may involve HUMINT under the form of undercover officer or entity performing physical surveillance to place bug on the device, use interception device or access a service provider in compliance with the laws or existing statutes of the respective law enforcement or intelligence agency. The later would require official request submitted to the service provider or just addressing the service provider directly and officially, as applicable and in accordance with existing agreements or country laws.

The Intelligence and Security Committee of the British Parliament has established that, even though advantageous, the interception of communication has various constraints. For instance, Service Providers in an effort to reduce cost and optimise business model may not keep data on the record of phone calls or messaging. Clients may

be accessing internet application through mobiles but the communication on these applications is not owned or known by the particular service provider. Communications between different jurisdictions may involve a number of service providers, meaning the data needed for the interception would be located on the servers of all these companies. Operators outside the EU may not have to comply with legal requirements to maintain data on the record or, even if they do, they may not be willing to share this with EU authorities.[67] This poses serious problems for law enforcement agencies, however, is still not of big concern for the intelligence community having additional "national security capabilities."

The main reason why law enforcement and intelligence agencies use SIGINT/ COMINT and HUMINT in countering TOC is its functioning in a denied type of environment. The access is limited, if not severely restricted – hence the need of high tech, undercover officers or recruited agents for infiltrating communication lines or group habitat. The infiltration of the TOC provides an opportunity also for countering terrorist groups since terrorists obtain resources, arms and information through other criminals. Additionally, terrorists make use of contraband and smuggling channels. While terrorists and organised crime groups have different modes of operation and motivations, they do rely on each other for services and goods. A terrorist group with paramilitary training may undertake paid operation on behalf of a crime group, as well a crime group may engage in a terrorist act in order to restrain, eliminate competition or assassinate a person for its personal interest or on behalf of a terrorist group. The interconnectedness between the two makes from the TOC's members valuable assets and treasure-troves of information on terrorists groups' links, needs, operations and senior members. Still, there are ethical concerns in terms of providing immunity from prosecution on criminals. Howard asserts that

> criminals particularly drug, arms and human traffickers could be a useful source of information and possibly actionable intelligence in the campaign against terrorism. This notion is timely because of a decision lifting restrictions imposed in 1995, which limited the opportunity for intelligence services to recruit informants who may have run afoul of human rights laws.[68]

Additionally, Howard points out that denied environments could be infiltrated by the recruited or volunteered members of specific ethnic communities or NGOs. The author rightfully notes the corresponding challenges in intelligence cooperation with NGOs,[69] however these mainly relate to the fight against terrorism because of political or human rights considerations and links with liberation movements. Nevertheless, countering TOC puts a different angle and the lack or refusal to cooperate with intelligence or law enforcement services may be considered an accessory to crime, naturally depending on national legislations.

Another area of TOC with particular specifics in building intelligence approaches is arm trafficking, especially when it refers to weapons of mass destruction (WMD). The interception of freights allegedly carrying WMD requires serious risk management considerations. While the sector of WMD sale and trafficking has been traditionally considered as reserved for national actors, Allen has remarked, "The emergence of proliferation networks, such as the lucrative multinational enterprise operated out of Pakistan by A. Q. Kahn, amply demonstrates that non-state actors now participate as both suppliers and consumers of WMD technology."[70] According to the author, the policymakers or authorities assigned to take responsibility for particular case dealing with WMD should be able to select workable approach that limits the risk in situations offering only negative outcomes. Meanwhile, these negative outcomes should be evaluated and the one coming with the bigger number of benefits should be selected as the way forward. Allen refers to the selection process among two erroneous choices as "the false positive error" and "the false negative error":

> Statistical decision theory recognises two types of inferential error. The false positive, or Type I, error refers to a conclusion that a condition exists or a proposition is true when in fact the condition does not exist or the proposition is not true. ... The false negative, or Type II, error is committed by concluding that a condition does not exist or that a proposition is not true when in fact the condition does exist or the proposition is true.[71]

As it has become obvious post 9/11, the ability to face converging threats has greatly improved through the performance of joint international operations not only in the strict field of law enforcement but also in the area of intelligence agencies.

The intelligence cooperation has domestic, interagency and international dimensions. For instance, apart from Interpol, a major US partner in countering transnational organised crime groups is the EU. The US have concluded cooperation agreements with EUROPOL[72] and EUROJUST.[73] EUROPOL is the EU's criminal intelligence agency. Some researchers reviewing its operational activities refer to it as the EU's FBI, however there is a difference. EUROPOL is an independent agency under the EU Commission and as such performs transnational intelligence gathering in Europe across sovereign and independent EU states.[74] EUROPOL collection activities are constrained to Europe, while the EU has another agency filling the vacuum in foreign intelligence gathering. This is the European Union Intelligence Centre (EU INTCEN) – a constituent part of the European External Action Service (EEAS), which is the EU Foreign Affairs' body. The EU has signed arrangements with the US in areas coming under the attention of the EU INTCEN, namely Justice and Home affairs and Non-proliferation cooperation. It is important to note that the EU INTCEN does not have a clandestine service and this fact relieves the centre from facing eventual and controversial sovereignty issues. Instead, it has directed intelligence gathering primarily to analysing Open Source Intelligence (OSINT) and IMINT coming from the

EU Satellite Centre or commercial providers. Further, it also receives all source intelligence through liaison or seconded officers from EU member countries.[75] In similar cases contributing countries maintain control over who sees the information and whether the collection methods are being identified.

The EU criminal intelligence agency EUROPOL is an evolving structure and, similarly to the EU, could be seen as constantly expanding its capabilities. One example is the joint 2011 initiative with Interpol in countering transnational organised crime groups on global level, building further on the regional European role of EUROPOL. Among the other aspects, the initiative arranges for secure exchange of information, analysis and operations planning.[76]

The data collected through the research indicates that following 9/11 there was substantial increase in joint international intelligence operations and the use of new liaison contacts for coordination purposes. The access to foreign sovereign territory or to information associated with the initial origins of a transnational organised crime group is facilitated by the cooperation with foreign intelligence services or police forces. The benefits are obvious. The foreign liaison improves analytical assessment in the area of local cultural understanding. Rosenbach and Peritz assert that cooperation offers the possibility for immediate access to intelligence or national security systems of other countries and helps in concealing the name or identity of the initial investigation or intelligence party.[77] On the negative side, and as experienced by the Czech Republic's counterintelligence agency BIS, their cooperation with foreign intelligence, Federal Security Service of the Russian Federation (FSB) in this case, in the field of police work and counter-terrorism was a cover for more succinct intelligence work on the territory of the country. Summarising the negatives, liaison may present adversaries with the possibility to explore unhindered intelligence gathering on foreign territory and give an insight on how national intelligence or security systems are functioning. Moreover, reliance on information coming from foreign intelligence liaison should be carefully weighed since countries have different standards in intelligence gathering, verifying sources and channels for collection. Last but not least, the ethics of intelligence collection and intelligence work play role in deciding whether to use a particular liaison (established or intended) or not.

The intelligence operations in countering transnational organised crime groups have also another particular specific that relates to the fact that some countries may approach members of their national communities abroad, who are engaged in illegal activities, and request their services in performing operations or tasks, thus concealing own participation. The incentives for involvement in such cooperation are coming under the form of motivating factors, use of violence or threat against families back home. This approach, noted by Magee, is typical for the ethnically driven recruitment done by non-state actors, being either terrorists or serious crime groups.[78] Therefore,

when approaching national authorities with request for investigation or intelligence support in pursuing transnational organised crimes committed by ethnically formed crime groups, from the domestic nationality, the requesting intelligence or law enforcement service should keep in mind the eventual constraints in receiving real or full support.

The same sentiment in addressing the international intelligence cooperation is shared by other researchers. Lefebvre defines intelligence cooperation as bilateral or multilateral.[79] Bilateral liaison is used for environments with difficult access, while the multilateral approach is typical for coalitions. UKUSA for instance is a multilateral cooperation among US and UK dating back to the Cold War, where US and UK have the status of first and Australia and New Zealand as second signatories.[80] This agreement is also known as the "Echelon." Rudner informs that, "later, countries like Denmark, Germany, and Turkey were reportedly included in a somewhat looser, more limited association as so-called 'Third Parties,' usually by virtue of bilateral arrangements with GCHQ (e.g. Sweden) or NSA (e.g. Norway)."[81]

Another example of multilateral intelligence cooperation is the Commonwealth of Independent States' Council of Directors of Security Agencies and Special Services, which meets regularly under the chairmanship of Russia's FSB, with a permanent coordination secretariat at the FSB's headquarters in Moscow. This entity involves the ex-Soviet countries of Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan. Lefebvre and McDermott assert that the cooperation is in the field of liaison, assistance in intelligence operations and intelligence sharing. It also focuses on countering radical religious groups, prevention of drug trafficking, dismantling separatist movements and securing government data.[82] Representative of the level of the threat faced by the Commonwealth of Independent States (CIS) in the fight against religious extremists, the CIS Council of Directors of Security Agencies and Special Services opened a Joint Counter-Terrorism Centre in Moscow in June 2000. Meanwhile, the Central Asian countries raised the importance of having local branches and the Moscow Centre opened a branch in Bishkek, Kyrgyzstan. Lefebvre and McDermott claim that following its establishment, the branch held meetings with the Central Intelligence Agency (CIA).

All available sources define the intelligence operations in countering transnational organised crime as a demanding endeavour, mostly because of the associated legal considerations and accompanying constraints. Legal challenges exist on local and international level. On local level we have issues related to the treatment and investigations of individuals in terms of interrogation tactics, electronic and physical surveillance and linked personal privacy, metadata, etc. The intelligence services of some countries apply different approaches when targeting local or foreign subjects. For in-

stance, the investigations of US persons, inside and outside of US, require permission from a Foreign Intelligence Surveillance Court (FISC). The permission is issued only if the government supports the relevance of its request through a written document indicating the possibility of participation in international terrorism or membership, affiliated with clandestine services.[83] The electronic surveillance of non-US persons does not require from the agencies to follow the FISC procedure, and that is valid for cases not only outside but also for investigations inside US.

Domestic investigation and electronic surveillance take place in an environment characterised with greater regulation, clear operational guidance and stringent oversight attention, including high publicity. On the other hand, the intelligence operations on foreign land are challenging and may cause political complications and decrease of trust among partners or important international counterparts. Stigall rightfully points to the issue of jurisdiction in international law as it relates to the pragmatics of countering transnational organised crime.[84] The author asserts that jurisdiction is directly linked to the sovereignty of a country or territory and the pursuit, investigation or apprehension of transnational organised crime group members or individuals on foreign soil contravenes the principle of sovereignty. Exceptions are possible only when the intelligence operation is undertaken in cooperation with the foreign authorities governing the jurisdiction or when these do not object or seek legal accommodation for the intervention in their sovereign matters.

The research points also towards increased use of military units in combating transnational organised crime or terrorism while exercising extraterritorial jurisdiction. The use of specialised military units does not always allow for due process in the manner typical for civilian law enforcement; meanwhile, the need to rely on military units could denote the severity of the surroundings conditions or a hostile environment. Stigall argues that, even if reasonable from national security point of view, similar involvement misdirects military units from their main tasks. The military tactics, rules of engagement and targeting differ greatly from the due process practices used by the civilian law enforcement because of their different statutory roles and environments of operations. On the other hand, and looking at the Law of Armed Conflict (LOAC), extraterritorial jurisdiction is not an option for civilian law enforcement. Only military units, under limited set of circumstances, nonetheless highly disputable, qualify for exercising extraterritorial jurisdiction under LOAC on a case by case basis. On many occasions the complexity and international challenges are such that an operation can never be repeated at a later point of time even if circumstances and conditions seem the same.

Mandel claims that nowadays the duties of the civilian law enforcement and the military are converging following the fusion of domestic with global security to the point of defining terrorism and transnational crime "as insurgency and crime control… as

low-intensity conflict."[85] Nonetheless, the risks associated with the military and civilian law enforcement intelligence operations in the area of countering transnational organised crime through the exercise of extraterritorial jurisdiction direct countries to the use of covert or clandestine operations. Covert and clandestine operations are neither less risky nor do they reduce political complications. Nevertheless, they are utilised by countries for effecting desired changes in foreign environments or for remaining under the radar. By definition and substance, these operations require greater oversight but this requisite differs from country to country and is parallel to the abilities of societies to participate in public life and engage in the exercise of personal liberties, whenever afforded by national legislation.

The changes in the two independent variables—international legal system and intelligence cooperation—affect the two dependent variables – prosecution in terms of improved results and increased number of joint international intelligence operations. The international legal system evolves slowly and it takes time for countries to agree on legal instruments having global application for various reasons, some related to sovereignty, and some to the effects on governments, caused by transnational crime.

The issue of cooperation and prosecution in multiple jurisdictions has also political nuances. For example, countries may agree easier on global legal measures against one or few particular transnational crimes while disagreeing on a common approach towards another. The inability of countries to find global agreement on prosecuting cybercrime is a proper illustration. In contrast, the international intelligence liaison in countering the global terrorism following 9/11 has increased significantly.

The increased intelligence cooperation has exposed foreign governments to new methods and tactics, and thus improved their efficiency in countering transnational organised crime groups and terrorism on strategic, operational and tactical levels. This trend is visible from the annual reports of national intelligence structures of the EU. Another finding from the gathered information is the militarisation of effort to counter TOC. Some of it relates to ungoverned spaces being used as bases for transnational organised crime groups, while others address crime groups infiltrating governments in weak countries, assuming control and maintaining law and order, or simply the possibilities for extraterritorial jurisdiction related to the LOAC. It is also possible to use militarised units to counter TOC groups due to tactical considerations.

The hypothesis is partially proven. Many countries do cooperate on issues related to transnational organised crime groups. Nonetheless, the cooperation may be limited to only one or few types of TOC. The fact that some countries may use the existing cooperation among civilian law enforcement agencies to perform intelligence gathering activities not linked to the field of actual cooperation is hampering, limiting or slowing down the progress in this direction. The cooperation among different countries will also depend on the ability of their intelligence services to collect profile data, in-

cluding personal and official relations on liaison counterparts in terms of individuals, structures, chain of command, access to information, sharing of information principles, information assurance practices and ability to maintain the intelligence liaison discreet and unexposed, depending on the task at hand.

The collected data indicates that the intelligence liaison in the field of countering transnational organised crime groups will be task or case based, interest oriented and will be strongly affected by political developments among partners or international counterparts. This signifies that, from a pragmatic perspective, the countering of the TOC on strategic level will focus on established relations within existing formats like NATO and EU and may involve the sanitisation of regions or weak countries affected by it; hence, the increased importance of specialised military units. It is evident that this approach would create legal complications and concerns in regard to following due process and respect for human rights. However, the absence of agreement among countries on global level aimed at limited and controlled execution of extraterritorial jurisdiction by civilian law enforcement agencies could direct policy-makers to choose the military option.

It is known that the reasons for the existence of organised crime cannot be eliminated only with the application of law enforcement or military instruments and would require instead the simultaneous application of strategic government programs in the field of human rights, education, sport, health, labour, taxation, social security, trade and commerce and foreign affairs. Nonetheless, this paper is focused merely on the aspects related to the application of intelligence operations in countering transnational organised crime groups.

* * *

> In the purest sense, intelligence is the end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a criminal phenomenon by using the scientific approach to problem solving (that is, analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.
>
> D. Carter [86]

Conclusion

The paper explored the legal considerations of intelligence operations in countering transnational organised crime groups. Reflecting upon the findings there are two main determinants shaping the underlying research. They are Intelligence Operations and TOC. These two factors exist in a global environment shaped by international relations, domestic, international politics and economies where international and national

actors, based on their cultural and social understanding, make decisions affecting social development and global discourse. International, regional and domestic legislations establish a procedural framework and thus could present "constraints" for the execution of intelligence operations in countering transnational organised crime.

The definition of "constraint" is mostly viewed from its negative connotation; nonetheless, international laws exist for good reason, creating order out of the initial chaos, and as such should be complied with, i.e. any eventual intelligence operation should be well justified, planned, properly authorised and precisely executed. The intelligence operations in countering transnational organised crime networks are performed by national intelligence or law enforcement agencies having either internal and external functions or only one of these two. The intelligence operations could have political colouring depending on governments, social development or politics. Apart from that governments may use ethnic elements from the crime contingents abroad for the execution of intelligence, covert or clandestine actions on foreign soils.

The TOC could be viewed as a fluctuating network, expanding or deserting cells depending on goals and pressing or accommodating authorities, meanwhile taking chances to profit from arbitrage possibilities in diverse countries having different legal and national security systems with the objective of providing goods and services to prospective clients willing to pay a higher price and assume certain risks. While most of the business networks comply with the laws and regulations in their area of operation, this is not that case with the transnational organised crime's networks which accumulate fast profits in short time and consider the ability to break and evade the law, find loopholes or infiltrate government services as a higher virtue. Besides, transnational organised crime groups do not have requirements for ethical conduct as is the case with any modern business or public service nowadays. Not only that but personnel in transnational organised crime groups is expendable in real terms; there are neither social schemes nor pension benefits for its members. The points above refer to the core and enforcing structures of criminal groups. Otherwise, it is understandable that many businesses may be owned by crime groups after accumulated illegal funds have been already laundered, and in fact these businesses owned by organised crime may be the strictest tax payers in the respective country.

The decision making process within the TOC groups is swift and free of political, bureaucratic or administrative constraints and considerations. Cost and well-being of group members is not important; attention is being paid to operational readiness and success. The challenges posed by the transnational organised crime groups are compounded by their constantly increasing budgets. The main problem of the TOC groups may be how to launder or invest the accumulated illegal profits. In contrast, the government agencies are constantly short of funds and compete for funding with

many other government programs that may be more attractive for policy-makers and groups of the electorate.

Many researchers have realised that the TOC networks could be countered only through coordinated global effort. Nevertheless, there are areas where countries agree and there are others, similar to cybercrime, where legal instruments from UN global level for example, are far from being agreed on. One exception is the Convention on Cybercrime issued by the Council of Europe in 2001. The lack of global legal instruments for civilian law enforcement and possibilities for the application of extraterritorial jurisdiction pushes modern democracies on the path of identifying group, block or regional methods in the fight with organised crime. By definition, this approach creates areas of stability where the rule of law is the prevailing approach, and areas of constant low intensity conflict where insurgent movements or transnational crime groups are active. Similar areas may be ruled by governments trying to step on the path of the rule of law or by such that utilise the moment to accomplish personal or group interests. Under these circumstances, it is understandable that on some occasions, intelligence operations on foreign soil may be handed over to military units, limiting the loss of life of unit members, limiting however also the scope of normal due procedures applied toward the targeted individuals, installations or processes.

For example in the US, the use of military units in intelligence operations for countering transnational organised crime groups is simultaneously applauded and disregarded. That is why civilian law enforcement agencies or foreign and national intelligence services still perform covert and clandestine operations. The reason for the performance of covert or clandestine operations may lay in the fact that a territory is not cooperating against specific "bases" and "businesses" or because specific public services are infiltrated by transnational organised crime groups.

The existence of cooperation agreements opens the way for joint international intelligence operations by removing the eventual legal challenges and political complications. On the other hand, there may be cases when a coordinated operation among two intelligence services may be interrupted by another local law enforcement agency performing its own surveillance. Sometimes, law enforcement agencies from one country do compete among each other for more respect, funding and hierarchical appreciation of activities. For example this was the case with the abduction of Abu Omar from Italy.[87] This case is also suggestive for the need of having proper operational planning and for avoiding the pitfalls that have brought it to the attention of the public in the first place: "The operatives used false names but left a paper trail of unencrypted cell phones records and credit card bills at luxury hotels in Milan."[88]

Putting aside the justification for Abu Omar abduction and focusing only on discussing its operational dimension, it becomes important to note that joint international intelligence operations should be taken seriously and the attention to detail should not

be negated because the operation takes place in an allied country. An ally allowing joint intelligence operation on its territory is exposed to domestic and political complications. For instance, in order to avoid such complications, mobile communications on foreign soil should be traversed through encrypted long distance stand-alone mobile radio units, independent from connection with the local mobile providers. At the end, abducting foreign nationals on foreign soil challenges international laws and their perception in various directions. Likewise, the abduction of General Noriega from Panama which was without a doubt performed in very different times and under very different international circumstances and settings was commented by Best:

> There is no question that such forcible abductions against the desires of a foreign country can greatly complicate U.S. relations with that country. Such efforts, according to some observers, appear to many in other countries to reflect U.S. disdain for acceptable procedures of international law. They arguably contribute to the impression that the U.S. relies on brute force and undermine legal norms. It is easy to imagine the public consternation in the U.S. if another country "snatched" a U.S. official and put him on trial.[89]

The option of executing clandestine or covert operations, combined with SIGINT, in countering transnational organised crime groups, and the use of undercover agents may be one of the feasible long term options within the current international legal format. Indeed, this would require strong oversight and authorisation mechanisms that should be both confidential and able to keep secure data on the record for the planned and undergoing intelligence operations. This confidential data will be secure only if the respective intelligence service or law enforcement agency is not infiltrated by the organised crime groups through corruption or another type of non-state actors' intelligence operations. Apart from non-state actors, the infiltration may be performed by "actors whose state controllers are not openly visible."[90] Therefore, it is important to carefully select the partners for joint international intelligence operations. This is also the reason for the existing tendency among national intelligence agencies to perform intelligence operations in hostile climates without involving international counterparts, allies or even national law enforcement structures, with the objective of protecting own sources and methods. For example, Best acknowledges that the information collected by the intelligence agencies may contain data pointing to illegal activities; still, this data may not be shared with law enforcement structures because sharing would indicate the specific methods and sources if submitted to the courts of law as evidence.[91]

Defining covert action, clandestine and undercover work as a major determinant in intelligence operations against transnational organised crime groups and the fact that we live in liberal democracies puts forward the necessity of proper intelligence oversight:

> In modern liberal democratic countries Intelligence and Security Agencies (I&S agencies) are widely accepted as being vital for defeating the forces that are threatening the very existence of the liberal democratic system. However the very task of these agencies implies a level of secrecy—and thus a relative lack of democratic transparency—because of their modus operandi, and the collection of information on individuals might easily impinge on individual rights.[92]

Future avenues for research of intelligence operations in countering transnational organised crime groups should expand and include the field of cognitive science in terms of mentally conditioning personnel for covert and undercover work. Furthermore, cognitive science will facilitate the development of psychological insights on the group psychology of crime group members from digitally recorded voice and facial analysis, as well as from Internet, social media and public behaviour, with the objective of achieving improved intelligence targeting. A particular opportunity for increased interception of serious organised crime groups' members may be presented within the EU as a result of the constant integration processes. The EU may research the effects of integration on countering transnational organised crime and the statutory possibilities for EUROPOL to engage in initiating and performing criminal intelligence operations on its own through EUROPOL personnel, across member countries, as well as to assume counterintelligence functions within the EU for all EU agencies, organisations and bodies.

Concluding the thesis, while taking under consideration the complex and constantly evolving nature of the subject, requiring pertinent updates; the paper ends with a quotation from Charles Darwin:

> Intelligence is based on how efficient a species became at doing the things they need to survive.

P.S. Update on the multilateral intelligence cooperation among the Directors of Security Agencies and Special Services of the Commonwealth of Independent States in the light of the 2014 events in Ukraine

The 34th session of the Council of the Directors of the Security Agencies and Special Services of the Commonwealth of Independent States took place on 15 May 2013 in Bishkek, Kyrgyzstan with the attendance of Azerbaijan, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russian Federation, Tajikistan, Uzbekistan and Ukraine. Representatives of the special services of the Federal Republic of Germany, the Italian Republic, the Kingdom of Spain and the French Republic have participated as observers.

The 35th session was held in Armenia on 18 October 2013. There is no information about the attending countries. The official press release on the website of the Armenian President comments briefly on the agenda:

> The Chairman of the Council, Director of RF Federal Security Service Alexander Bortnikov assessed the works of the Council of the Heads of the CIS security agencies and special services in Tsakhkadzor as well as all previous meetings as efficient and noted that cooperation of the member states in the framework of the Council aimed at countering threats existing in the contemporary world such as terrorism, drug trafficking, organised crime and many other dangerous activities is developing dynamically. He also stressed the importance of experience exchange between the countries and works related to the synchronisation of the legislations of the member states.

The 36th session has gathered participants on 5 June 2014 in Belarus. Georgia did not participate, as the country is no longer a member of the CIS. Germany, Italy, Spain and France have again been invited but it is not clear whether their representatives attended this session. The official press-release on the website of the President of Belarus notes that Ukraine had announced plans to follow Georgia in leaving the CIS. However, the press release is not informing if this message was delivered in person by a Ukrainian representative or it was submitted through official correspondence. Additionally, it reports that "Alexander Lukashenko is convinced that in the CIS format it is the CIS security services that are expected to identify collective security risks, challenges and threats and create pre-conditions for smooth and successful development of the Commonwealth and each member state in particular. This development should be progressive and smooth, without a shocking therapy and social distress" and cites the words of the President of Belarus:

> We should not expect other countries to provide us with efficient recipes of countering challenges and threats of regional security. We are responsible for the stability in our land and we should come up with joint mechanisms to respond to destabilising factors.

The Council also reports a share of its activities under the format of the Counterterrorism Committee at the United Nations Security Council. The latest such report was issued on 23 January 2014. It was presented by the Head of the Department of International Cooperation and Deputy Head of the Federal Security Service of the Russian Federation, A.F. Kuzyura.

Acknowledgement

This article is short version of a Master Thesis in Intelligence Studies, defended at the American Military University in Washington, DC.

Notes

[1] UNODC, "United Nations Convention against Transnational Organised Crime and the Protocols Thereto," accessed January 8, 2014, www.unodc.org/unodc/en/treaties/CTOC/index.html.

[2] UNODC, "The Globalization of Crime. A Transnational Organised Crime Threat Assessment," 2011, http://www.unodc.org/documents/organised-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf.

[3] US Department of Justice, "Overview of the Law Enforcement Strategy to Combat International Organized Crime," 2008, http://www.justice.gov/sites/default/files/ag/legacy/2008/04/23/ioc-strategy-public-overview.pdf.

[4] US Department of Justice, Overview of the Law Enforcement Strategy to Combat International Organized Crime.

[5] EUROPOL, "SOCTA 2013 EU Serious and Organised Crime Threat Assessment," 2013, www.europol.europa.eu/sites/default/files/publications/socta2013.pdf.

[6] Gregory F. Treverton, "Intelligence, Law Enforcement, and Homeland Security," The Century Foundation, Homeland Security Project, 2002, http://72.32.39.237:8080/Plone/publications/2002/8/pb278.

[7] Michael D. Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, D.C.: National Defense Intelligence College, 2010), http://www.ni-u.edu/ni_press/pdf/The_Blue_Planet.pdf.

[8] Johns Rollins and Liana Sun Wyler, "Terrorism and Transnational Crime: Foreign Policy Issues for Congress," Congressional Research Service, 2012, 6, available at http://www.refworld.org/docid/51d53c354.html.

[9] EUROPOL, "OCTA EU Organised Crime Threat Assessment," 2011, 8, https://www.europol.europa.eu/sites/default/files/publications/octa_2011_1.pdf.

[10] James Bergeron, "Transnational Organised Crime and International Security," *The RUSI Journal* 158, no. 2 (2013): 6-9, quote on p. 6, http://dx.doi.org/10.1080/03071847.2013.787728.

[11] Michael C. Kenney, "Intelligence Games: Comparing the Intelligence Capabilities of Law Enforcement Agencies and Drug Trafficking Enterprises," *International Journal of Intelligence and CounterIntelligence* 16, no. 2 (2003): 212-243, quote on p. 213, available at http://dx.doi.org/10.1080/08850600390198733.

[12] Carl Anthony Wege, "Hizballah's Counterintelligence Apparatus," *International Journal of Intelligence and CounterIntelligence*, 2012, 777.

[13] Michael Braun, David Asher and Matthew Levitt, "Party of Fraud: Hizballah's Criminal Enterprises," *PolicyWatch 1911*, 2012.

[14] Glen M. Segell, "Intelligence Agency Relations Between the European Union and the U.S," *International Journal of Intelligence and CounterIntelligence* 17, no. 1 (2004): 81-96, quote on p. 82, available at http://dx.doi.org/10.1080/08850600490252678.

[15] James Cockayne, "Transnational Organized Crime: Multilateral Responses to a Rising Threat," *Coping with Crisis Working Paper Series*, International Peace Academy, 2007, 2.

[16] Cockayne, "Transnational Organized Crime: Multilateral Responses to a Rising Threat."

[17] Cockayne, "Transnational Organized Crime: Multilateral Responses to a Rising Threat."

[18] Mark Shaw, "Typologies of Transnational Organized Crime Groups," Centre for International Crime Prevention, UNODC, accessed February 12, 2014, www.unodc.org/pdf/crime/training/typologies.pdf.

[19] UNODC, "Criminal Intelligence Manual for Analysts," United Nations Publications, 2011, www.unodc.org/documents/ organised-crime/Law-enforcement/Criminal_Intelligence_for_Analysts.pdf.

[20] UNODC, "Criminal Intelligence Manual for Analysts."

[21] UNODC, "Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime," United Nations Publications, 2009, www.unodc.org/documents/organised-crime/Law-Enforcement/Electronic_surveillance.pdf

[22] Jharna Chatterjee, *The Changing Structure of Organised Crime Groups*, Research and Evaluation Branch, Community, Contract and Aboriginal Policing Services Directorate, Royal Canadian Mounted Police, 2005.

[23] UNODC, "Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries," United Nations Publications, 2002, https://www.unodc.org/pdf/crime/publications/Pilot_survey.pdf.

[24] Carlo Morselli, Thomas Gabor and John Kiedrowski, *The Factors That Shape Organized Crime*, Research and National Coordination, Organized Crime Division, Law Enforcement and Policy Branch, Public Safety Canada, 2010.

[25] Morselli, Gabor and Kiedrowski, *The Factors That Shape Organized Crime.*

[26] Tom Lansford, "Multinational Intelligence Cooperation," in *Countering Terrorism and Insurgency in the 21st Century: International Perspectives Volume 1: Strategic and Tactical Considerations*, ed. James J.F. Forest (Westport, CT: Praeger Publishers, 2007).

[27] Erik Nemeth, "Art-Intelligence Programs: The Relevance of the Clandestine Art World to Foreign Intelligence," *International Journal of Intelligence and CounterIntelligence* 21, no. 2 (2008): 355-374, quote on p. 365, http://dx.doi.org/10.1080/08850600701854441.

[28] Nemeth, "Art-Intelligence Programs."

[29] Isabel Kershen, "Israel Says It Seised Iranian Shipment of Rockets Headed for Gaza," *New York Times*, accessed February 12, 2014, www.nytimes.com/2014/03/06/world/middleeast/israel-says-it-seised-iranian-shipment-of-rockets-headed-for-gaza.html?_r=1.

[30] Gary Cordner & Kathryn Scarborough, *Connecting Police Intelligence with Military and National Intelligence in Homeland Security and Intelligence* (Westport, CT: Praeger, 2010).

[31] Guaracy Mingardi, *"*The Role of Intelligence Work in the Control of Organized Crime,*"* translated by Jeffrey Hoff, *Estudos Avancados*, 2007, 55, accessed February 12, 2014, http://www.scielo.br/scielo.php?script=sci_abstract&pid=S0103-40142007000300004&lng=pt&nrm=iso&tlng=en.

[32] Yvon Dandurand, *Strategies and Practical Measures to Strengthen the Capacity of Prosecution Services in Dealing with Transnational Organised Crime, Terrorism and Corruption* (Crime Law Soc Change, Springer Science + Business Media B.V., 2007), 226.

[33] Marshal Curtis Erwin, "Covert Action: Legislative Background and Possible Policy Questions," Congressional Research Service Report for Congress, 2013, available at http://fas.org/sgp/crs/intel/RL33715.pdf.

[34] Richard J. Aldrich, "Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem," *Intelligence and National Security* 24, no. 1 (2009): 26-56, quote on p. 33, http://dx.doi.org/10.1080/02684520902756812.

[35] Segell, "Intelligence Agency Relations Between the European Union and the U.S," 86.

[36] Federal Ministry of the Interior, "Annual Report on the Protection of the Constitution. Summary," 2013, http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2013/vsb_kurzfassung_engl_2012.pdf?__blob=publicationFile.

[37] Bundeskriminalamt, "Organised Crime National Situation Report 2011," 2011.

[38] Security Information Service, "Annual Report of the Security Information Service for 2012," http://bis.cz/n/ar2012en.pdf.

[39] Internal Security Agency, "Annual Report 2009," 2009, https://www.abw.gov.pl/download/2/620/ANNUALREPORT2009.pdf.

[40] Danish Security and Intelligence Service, "Report 2008-2010," 2011, https://www.pet.dk/English/~/media/Engelsk/PETBeretning20082010UKpdf.ashx.

[41] The Egmont Group Secretariat, "2011-2012 Annual Report," 2012, http://www.egmontgroup.org/library/download/233.

[42] Federal Office of Police, "2012 Annual Report by the Money Laundering Reporting Office Switzerland MROS," 2012, 82, http://www.fedpol.admin.ch/dam/data/kriminalitaet/geldwaescherei/jb/jb-mros-2012-e.pdf.

[43] Joseph W. Wippl, "Intelligence Exchange through InterIntel," *International Journal of Intelligence and CounterIntelligence* 25, no. 1 (2012): 1-18, quote on p. 8, available at http://dx.doi.org/10.1080/08850607.2011.598782.

[44] Wippl, "Intelligence Exchange through InterIntel."

[45] Elisabeth Symeonidou-Kastanidou, "Towards a New Definition of Organised Crime in the European Union," *European Journal of Crime, Criminal Law and Criminal Justice* 15, no. 1 (2007): 83-103, quote on p. 84.

[46] David E. Pozen, "The Mosaic Theory, National Security, and the Freedom of Information Act," *Yale Law Journal* 115 (2005): 628-279, quote on p. 630.

[47] University of Southern California Libraries, "Organizing Your Social Sciences Research Paper. Methodology," accessed February 22, 2014, http://libguides.usc.edu/content.php?pid=83009&sid=615866.

[48] Carl Gustav Jung, *The Archetypes and the Collective Unconscious*, ed. Richard Francis Carrington Hull (Princeton, NJ: Princeton University Press, 1959), 3.

[49] Barney G. Glaser and Anselm L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research* (New Brunswick and London: Aldine TransAction, 1967), 238.

[50] Web Center for Social Research Methods, "Qualitative methods. Research Methods Knowledge Base," accessed February 22, 2014, www.socialresearchmethods.net/kb/qualapp.php.

[51] Allison Jamieson, "Cooperation between Organized Crime Groups around the World", Research Institute for the Study of Conflict and Terrorism, 1999, 13, accessed February 22, 2014, http://www.bmlv.gv.at/wissen-forschung/publikationen/beitrag.php?id=812.

[52] Adam D.M. Svendsen, "Connecting Intelligence and Theory: Intelligence Liaison and International Relations," *Intelligence and National Security* 24, no. 5 (2009): 700-729, quote on p. 701, available at http://dx.doi.org/10.1080/02684520903209456.

[53] Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence* 1, no. 1 (1955), 4.

[54] RIEAS, "Memorandum of Cooperation between the Mediterranean Council for Intelligence Studies (MCIS) and with the Center for Intelligence Studies, University of Calabria, Italy," 2010, accessed February 22, 2014, www.rieas.gr/blog/1154-memorandum-of-cooperation-between-the-mediterranean-council-for-intelligence-studies-mcis-and-with-the-center-for-intelligence-studies-university-of-calabria-italy-.html.

[55] David M. Luna, "Fighting Networks with Networks," in *Convergence: Illicit Networks and National Security in the Age of Globalization*, ed. Michael Miklaucic and Jacqueline

Brewer (Washington, DC: National Defense University Press, 2013), 213-232, quote on 213, available at http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=163849.

[56] White House Administration, "Strategy to Combat Transnational Organised Crime. Addressing Converging Threats to National Security", 2011, 1, www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organised_Crime_July_2011.pdf.

[57] Michael Miklaucic and Jacqueline Brewer, eds., *Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense University Press, 2013), http://www.ndufoundation.org/file/pdf-test/Convergence.pdf.

[58] White House Administration, "Strategy to Combat Transnational Organized Crime."

[59] Marilyn Peterson, "Intelligence-Led Policing: The New Intelligence Architecture," Bureau of Justice Assistance, Department of Justice, 2005, http://www.ncjrs.gov/pdffiles1/bja/210681.pdf.

[60] Howard Abadinsky, *Organized Crime* (Belmont, CA: Wadsworth, 2010), 399.

[61] Guaracy Mingardi, "The Role of Intelligence Work in the Control of Organised Crime," 55.

[62] EurActiv, "EU Nations Developing Cyber 'Capabilities' to Infiltrate Government, Private Targets," 2013, accessed March 1, 2014, http://www.euractiv.com/infosociety/eu-nations-lack-common-approach-news-532294.

[63] The Financial Action Task Force, "Best Practices Paper. Sharing among Domestic Competent Authorities. Information Related to the Financing of Proliferation," 2012, 6, accessed March 1, 2014, www.fatf-gafi.org.

[64] The Financial Action Task Force, "Best Practices Paper."

[65] Peter Bell and Mitchell Congram, "Communication Interception Technology (CIT) and its use in the Fight against Transnational Organised Crime (TOC) in Australia: A Review of the Literature," *International Journal of Social Science Research* 2, no. 1 (2014): 46-66, quote on p. 59, http://dx.doi.org/10.5296/ijssr.v2i1.4089.

[66] Bell and Congram, "Communication Interception Technology."

[67] Malcolm Rifkind, MP, "Access to Communications Data by the Intelligence and Security Agencies," Intelligence and Security Committee, British Parliament, 2013, 11.

[68] Russell D. Howard, *Intelligence in Denied Areas: New Concepts for a Changing Security Environment* (The Joint Special Operations University Press, 2007), 7.

[69] Russell D. Howard, *Intelligence in Denied Areas*, 25.

[70] Craig H. Allen, *Maritime Counterproliferation Operations and the Rule of Law* (Westport, CT: Praeger, 2007).

[71] Craig H. Allen, *Maritime Counterproliferation Operations and the Rule of Law*.

[72] EUROPOL, "Europol Activities (Agreements)," 2012, accessed March 1, 2014, https://www.europol.europa.eu/content/europol-review-2012.

[73] EUROJUST, "EUROJUST-US Agreement," 2006, accessed March 1, 2014, eurojust.europa.eu/about/legal-framework/Pages/eurojust-legal-framework.aspx#partners.

[74] Segell, "Intelligence Agency Relations Between the European Union and the U.S.," 91.

[75] Maia K. Davies Cross, "A European Transgovernmental Intelligence Network and the Role of IntCen," Perspectives on European Politics and Society, ARENA Centre for European Studies, 2014, 389.

[76] EUROPOL, "EUROPOL-INTERPOL Agreement," 2011, accessed March 1, 2014, https://www.europol.europa.eu/content/press/interpol-and-europol-agree-joint-initiatives-enhance-global-response-against-transnati.

[77] Eric Rosenbach and Aki J. Peritz, "Confrontation or Collaboration? Congress and the Intelligence Community. Background Memos on the Intelligence Community Report," Belfer Center for Science and International Affairs, Harvard Kennedy School, 2009, 1.

[78] Aden C. Magee, "Countering Nontraditional HUMINT Collection Threats," *International Journal of Intelligence and CounterIntelligence* 23, no. 3 (2010): 509-520, quote on p. 516, available at http://dx.doi.org/10.1080/08850601003798807.

[79] Stephane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 527-542, quote on p. 529, http://dx.doi.or/10.1080/716100467.

[80] Lefebvre, *"The Difficulties and Dilemmas of International Intelligence Cooperation."*

[81] Martin Rudner, "Britain Betwixt and Between: UK SIGINT Alliance Strategy's Transatlantic and European Connections," *Intelligence and National Security* 19, no. 4 (2004): 571-609, quote on p. 577, http://dx.doi.org/10.1080/0268452042000327528.

[82] Stephane Lefebvre and Roger N. McDermott, "Russia and the Intelligence Services of Central Asia," *International Journal of Intelligence and CounterIntelligence* 21, no. 2 (2008): 251-301, quote on p. 259, http://dx.doi.org/10.1080/08850600701648678.

[83] Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire, "Liberty and Security in a Changing World," Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 2013, 81.

[84] Dan E. Stigall, "Ungoverned Spaces, Transnational Crime, and the Prohibition on Extra-territorial Enforcement Jurisdiction in International Law," *Selected Works of Dan E. Stigall* (2013), 19, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2211219.

[85] Robert Mandel, "Dark Logic: Transnational Criminal Tactics and Global Security," Stanford Security Studies (2011), 168.

[86] David L. Carter, "Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies," Second Edition, U.S. Department of Justice. Office of Community Oriented Policing Services, 2009, 9.

[87] FOX News, "Ex-CIA agent convicted of Italian kidnapping and held in Panama returning to US," 2013, accessed March 22, 2014, http://www.foxnews.com/world/2013/07/19/italy-ex-cia-chief-convicted-in-milan-in-kidnapping-muslim-cleric-is-detained/.

[88] Rachel Donadio, "Italy Convicts 23 Americans for C.I.A. Renditions," *New York Times*, November 4, 2009, accessed March 22, 2014, http://www.nytimes.com/2009/11/05/world/europe/05italy.html.

[89] Richard A. Best Jr., "Intelligence and Law Enforcement: Countering Transnational Threats to the U.S," Congressional Research Service Report for Congress, 2001, 26, available at http://fas.org/irp/crs/RL30252.pdf.

[90] Paul Medhurst, Professor at American Military University (2014).

[91] Richard A. Best Jr., "Intelligence and Law Enforcement: Countering Transnational Threats to the U.S."

[92] Ybo Buruma, "Accountability for Human Rights in the World of Intelligence. Some Tentative Conclusions," Law Faculty of the Radboud University, The Netherlands, International Symposium, 2007, available at http://hdl.handle.net/2066/38117.

Yavor Ivanov DINEV is a recent graduate from the American Military University in Washington, DC with Master of Arts in Intelligence Studies with Honors Degree. His educational background includes an MBA, MSc and two postgraduate diplomas. The author is a member of the International Association of Law Enforcement Intelligence Analysts (IALEIA), Armed Forces Communication and Electronics Association International (AFCEA), Austrian Centre for Intelligence, Propaganda and Security Studies with Karl Franzen University, Graz (ACIPSS) and the International Society of Political Psychology (ISPP). His main work experience is with the field missions of international organisations while his military service was with the airborne units of the Bulgarian military.