The general model of counter-terrorism

József Beke

Ministry of Foreign Affairs and Trade, Budapest, Hungary
Consulate General of Hungary in Innsbruck, Austria
E-mail: jozsef.beke@gmail.com

Received: 30 January 2023; accepted: 13 March 2023

Summary

One of the very important conditions for the normal functioning of a state is its ability to defend itself against various external or internal threats, attacks, and dangers. Such security challenges may be e.g. natural disasters, health emergencies, external attacks (military, political, economic), economic collapse, civil strife, organised crime, terrorism, etc. A well-functioning state has the appropriate administrative, health, law enforcement, military, etc. organisations, and structures to deal with and respond to these types of challenges and threats.

There are several studies in the literature (both Hungarian and foreign) on the theoretical model of intelligence services. Without exception, these theories take the approach of constructing a theoretical model through the various activities of secret services. In this paper, I attempt to construct, albeit sketchily, a kind of general, logical-functional counter-terrorism model to illustrate the complex activities of counter-terrorism intelligence and law enforcement organisations.

Keywords: terrorism, state security, counter-terrorism, police, law enforcement, secret service

A terrorelhárítás elméleti modellje

Beke József

Külgazdasági és Külügyminisztérium, Budapest, Magyarország
Magyarország Főkonzulátusa, Innsbruck, Ausztria

Összefoglalás

Az államok normális működésének egyik nagyon fontos feltétele, hogy az állam önmagát képes legyen megvédeni különböző külső vagy belső fenyegetésektől, támadásoktól és veszélyektől. Ilyen biztonsági kihívások lehetnek pl. természeti katasztrófák, egészségügyi veszélyhelyzet, külső támadás (katonai, politikai, gazdasági), gazdasági összeomlás, belviszály/polgárháború, szervezett bűnözés, terrorizmus stb. Egy jól működő állam esetében megvannak a megfelelő államigazgatási, egészségügyi, rendészeti, katonai stb. szervezetek és strukturák az ilyen típusú kihívások és veszélyhelyzetek kezelésére, megszüntetésére. Jelen tanulmány szempontjából alapvetően a terrorizmus releváns biztonsági kihívás, ennek megfelelően az erre adott állami választ, a terrorelhárítás egy lehetséges elméleti modelljét állítom fel és mutatom be vázlatosan, annak titkosszolgálati és rendőrségi szempontjai szerint.

A nemzetbiztonsági szolgálatok működésének alapját a történelmük során mindig speciális feladatrendszerük, az állam területi integritásának biztosítása, függetlenségének és állampolgárai jogainak és biztonságának a védelme határozta meg *(Boda–Regényi 2019)*. Ezeknek a feladatoknak az ellátásához a szolgálatok törvényi felhatalmazással különleges eszközöket és módszereket használhatnak és használnak. A titkosszolgálatok működési területük alapján két csoportra, polgári és katonai szolgálatokra oszthatók, míg a klasszikus szakmai tevékenységi körük alapján hírszerző és elhárító feladatokat láthatnak el *(Dávid 2018: 15)*. Már ez alapján is világosan látszik, hogy a szolgálatok szerepe és feladatköre mennyire szerteágazó és sokszínű lehet. A terrorizmus elleni küzdelem pedig ennek a feladatnak csak egy, bár kétségkívül nagyon fontos része. A szakirodalomban (magyar és külföldi egyaránt) több tanulmány is foglalkozik a titkosszolgálatok elméleti modelljével. Ezek az elméletek kivétel nélkül azt a megközelítést használják, hogy a titkosszolgálatok egyes tevékenységi körein keresztül állítják fel az elméleti modellt. Jelen tanulmányban arra vállalkozom, hogy – ha vázlatosan is – de megalkossak egyfajta általános, logikai-funkcionális terrorelhárítási modellt, a terrorelhárítást végző elhárító és rendészeti szervezetek összetett tevékenységének bemutatására.

Kulcsszavak: terrorizmus, nemzetbiztonság, terrorelhárítás, rendőrség, rendészet, titkosszolgálat

Introduction

Terrorism as a social phenomenon is very difficult to define in a precise and uniform way. It is therefore not surprising that the fight against terrorism is not easy to define. To put it simply, counter-terrorism can be defined as the activities against terrorism, terrorists, and the methods, means, and procedures used to combat them.

In this approach, counter-terrorism is essentially (but not exclusively!) a set of measures and methods of a defensive nature. Such means may include, for example, reconnaissance, usually carried out by national/state security services or police units, but also the prevention or interruption of a terrorist act, and the apprehension of the perpetrators. It follows that the fundamental aim of counter-terrorism is not primarily to destroy terrorists, but to disrupt and dismantle a terrorist act, gather evidence, apprehend the perpetrators, prosecute them and bring them to justice. Counter-terrorism has also become widespread in legislative practice and is therefore also used preferentially (although not exclusively) in the drafting of laws to prevent terrorism or to deal with terrorist situations. It is also used to organise measures for the protection of various priority sites and critical infrastructures, obviously in the context of counter-terrorism and the prevention of terrorist attacks.

There are states where counter-terrorism tasks fall within the competence of the army. Accordingly, counter-terrorism can be understood as active action against terrorists or terrorism, primarily military operations of an offensive nature (in practice, so-called low-intensity) *(Kőszegvári 2002)*. In military operations, the aim is often (not exclusively!) to physically destroy terrorists and not to ensure that criminal prosecutions are brought. Accordingly, the devices, methods, and tactics used are essentially designed to achieve this objective. In my view, a distinction must be made between military and law enforcement methods in the fight against terrorism. This point of view is also supported by Géza Finszter, who argues that it is wrong to use the dangers posed as an excuse to distinguish between military and law enforcement interventions. The perception of the crime (terrorism) as a declaration of war relieves states of the burden of proof and makes or may make the use of retaliatory measures unlimited. Great power with sufficient military power can do this, but the consequences are certainly worrying. However, the rule of law principles of action, necessity, and proportionality, should not limit the extent of covert interventions because of the magnitude of the threat. This would inevitably entail a violation of the civic integrity of the civilian community *(Finszter 2002: 156–166)*. Rights organisations also oppose the use of military force, means, and methods for counter-terrorism purposes because human rights issues are more difficult to address. They are thinking here of the rights of the captured terrorist. It is therefore very different whether he is given the status of a prisoner and, for example, prosecuted, or whether he is held in a quasi-title situation and subjected to a 'military security procedure', deprived of the possibility of legal defense *(Hautzinger 2006: 33–43)*.

Defensive or offensive counter-terrorism

Each State shall carry out the detection and countering of terrorist threats, and the monitoring (operational processing) of previously identified terrorist organisations and persons associated with terrorism when there are reasonable grounds to believe that they are planning, attempting, or committing terrorist acts or otherwise pose a threat to society or the functioning of the State. Such activities, which are primarily preventive in nature, can only be carried out if the operational processing of persons linked to terrorism and the performance of law enforcement tasks related to the terrorist threat posed by terrorist organisations, their potential targets, and persons targeted are carried out continuously. It can therefore be seen that counter-terrorism is a constantly evolving field, which operates and applies its specific tools to carry out its tasks in the current political, social, and security environment. The objectives to be achieved determine whether counter-terrorism is a defensive or offensive activity.

Defensive counter-terrorism devices and methods are primarily used when terrorist intentions against the state or its citizens are still covert and not overt. In other words, it is essentially a defensive counter-terrorist activity whose primary objective is prevention.

Offensive counter-terrorism is a set of devices and methods to actively target and counter an already detected terrorist threat or effort *(Dávid 2018: 171)*. This includes the eradication mentioned above and carried out by the police. In addition to compliance with the law, eradication may also involve the use of coercive means (legitimate physical violence). However, the aim is still not to destroy the perpetrators, but rather to interrupt the terrorist act, apprehend the terrorists, and ensure that criminal proceedings are initiated.

The three levels of counter-terrorism

The international literature distinguishes three levels of counter-terrorism: tactical, operational, and strategic *(Maras 2016: 242)*.

The tactical level is defined as the level at which counter-terrorism activities are aimed at preventing, disrupting, or eradicating a planned or initiated terrorist act. It includes all counter-terrorism activities aimed at preventing a terrorist or terrorist organisation from obtaining weapons, material support, entering the country, moving freely to achieve their objectives, etc.

The operational level of counter-terrorism is the set of social and governmental measures that can be taken to reduce and prevent the threat of terrorism. This includes measures and legal obligations that are effective means

of detecting and controlling the financing, harmful propaganda, and recruitment activities of terrorism. A very important element of this level is the continuous international cooperation and exchange of information in the fight against terrorism. The most effective way of depriving a terrorist or terrorist organisation of their support and the logistical base is at the operational level. In this way, we can ensure that the terrorist has no opportunity to commit his act. Here we must also turn to the online space for thought. In counter-terrorism circles, since the Internet became commonplace, it has become a well-known fact that terrorists use the web for psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilisation, networking, information sharing, planning, and coordination *(Weimann 2004: 5–10)*. Therefore, new approaches to these new types of challenges, such as security awareness, national security, and law enforcement sectors can certainly provide an adequate response. In particular, it calls for a significantly different approach from previous counter-terrorism practices, and a broader, more open relationship with the international professional community and society, rather than the narrow, skillful conspiratorial cooperation of the past *(Nagy–Mezei 2020: 50)*.

The terrorists' aim is usually to achieve or even enhance the secondary, psychological effect of their actions, which can influence public opinion and political decisions. They seek to use this secondary effect to strengthen their own position and to build or broaden their social support and base. At the strategic level of counter-terrorism, the aim is to make it clear to terrorists that their activities are not hidden from the counter-terrorism services, that they cannot achieve their objectives, and that their actions do not have public support. It is the effective application of the previous two levels that make the strategic level truly effective *(Maras 2016: 242–248)*.

Options for obtaining information on counter-terrorism

One of the most important tasks of counter-terrorism is to collect, analyse and assess information on terrorism. It is therefore not surprising that all counter-terrorism services strive to build up the broadest possible information-gathering capabilities, using the full range of information-gathering methods. Services can obtain the information they need to operate and carry out their tasks essentially from open or secret sources or by using tools and methods. The scope of open-source intelligence (OSINT) includes virtually all sources of information that are accessible to the public. This can include, for example, electronic and printed media, books, conferences, scientific lectures, religious events and rituals, social media platforms (Facebook, Twitter, Instagram, Tiktok), etc. The advantage of this method is that it does not require external authorisation (from a judge, prosecutor, or minister) and there is little risk of deconspiration. The disadvantage is that it is often difficult to verify the source or veracity of the data and therefore requires much more in-depth analysis and processing. It can be seen from the above that the most important and fundamental purpose of OSINT is to support counter-terrorism objectives with its own specific and innovative tools, as part of and complementary to traditional intelligence activities.

Intelligence gathering is a collection term with many definitions and interpretations in the literature. The most common definition of this activity is the collection of data and information by organisations authorised by law, to carry out tasks defined by law, by using forces, means, and methods capable of restricting the rights to the inviolability of private property, private and archival privacy, the protection of personal data and the protection of property, without the knowledge of the person concerned. In the public consciousness, the term has become intertwined with the term 'secret services', which is reflected in the very terminology used, since the various secret services (national security, state security) carry out their tasks in secret, in secret activities, away from the public at large *(Dobák 2018: 103)*.

One of the oldest intelligence-gathering methods is human intelligence, known in the trade as HUMINT. In all cases, humans are at the center of this type of intelligence gathering. It follows that the method is used only and exclusively to obtain information that the 'source' possesses or has access to. One of the great advantages of the method is that information can be obtained which has not yet been described by the data holders, thus making plans, ideas, and opinions available. Another major advantage is its flexibility since if a HUMINT source cannot obtain a piece of data, it is possible to search for a new source immediately or in parallel *(Dávid 2018: 120)*. Counter-terrorism experience in recent years has shown that the role of HUMINT in intelligence gathering has been reassessed, given the reluctance of terrorists to use the communication and contact possibilities offered by IT devices. They are aware that the electrotechnical detection capabilities of the counter-terrorist services can control all technical means/devices of information flow.

Among the information-gathering capabilities of the counter-terrorism services, the collection of data through electrotechnical means of detection, known as SIGINT (signals intelligence), is a prominent one. It is a complex intelligence-gathering activity involving several tools and methods. Among these, the most prominent is the collection of information through communication intelligence (COMINT), often colloquially referred to as telephone interception. In the fight against terrorism, this technical form of information collection is essentially understood as the channels and forms of communication that can be used by terrorists who are among the peaceful members of society (e.g. mobile phones and internet-based communication services) *(Dobák 2017)*. The ad-

vantage of this method is that the intercepted conversations can be well recorded and, if implemented correctly, the risk of deconspiration is minimal. The drawback is that manufacturers or service providers are improving the tools and methods used to protect information devices and channels, which are becoming increasingly difficult to crack. It is a common saying in professional circles that while before the info-communications "revolution" the question in covert intelligence gathering was how to open a lock or how to enter a building undetected by using a method and tactics, today the most important question is how to break into communication applications and mailboxes. A further disadvantage is that if the target knows or suspects that he is being intercepted, he can immediately switch to another communication channel or deliberately mislead the counter-terrorism service with his communications.

Analytical-assessment work in counter-terrorism

In the vast majority of cases, the data obtained using the tools and methods described above do not immediately constitute information in themselves. This is where the process of aggregating and processing a large amount of data to extract information relevant to counter-terrorism comes in. This process is called data processing and is carried out either directly by the "case manager" or, in most cases, by specially trained analysts/evaluators. The key objective at this stage is to enable the analyst assessors to process as much relevant information as possible and subsequently use it to prevent or disrupt terrorist attacks. In terrorism-related cases, it is often the case that the analysis of data requires specialised knowledge, in particular language skills (Arabic, Pashto, Urdu, Persian, etc.) and religious and cultural knowledge. There are three main methods of analysis and evaluation used by professionals.

The first method is to use simple logical laws and rules to extract the information required. This may include but is not limited to simple comparisons, flow charts, analysis of networks of contacts, or even profiling. The method chosen will, of course, depend to a large extent on the type of data to be analysed and the objective to be achieved. The next method is the so-called bounded analytical evaluation procedure, where a person or event related to a given terrorism is evaluated in the same or similar system in each case. This may include different risk analyses (either personal or critical infrastructure) or biographies, financial or banking records, and passenger name records (PNR). The advantage of this method is that all users or customers receive the same information in a tied procedure. This is also one of the most important conditions for the efficient use of the method. The third method is the so-called complex analysis and evaluation model. The method itself means that methodologies developed in different scientific fields and their results are transferred to the counter-terrorism field. Consequently, this method is more time-consuming and requires a higher level of professionalism on the part of the analysts. This includes scientific methods such as graph theory, game theory, matrix theory, etc. *(Dávid 2018: 122–125)*.

The analysis and evaluation of information involve drawing conclusions and evaluations, and making forecasts, sometimes even possible scenarios. The models and methods described above help analysts draw the appropriate conclusions from the available information and develop assessments. The evaluations are useful for users (political, economic, law enforcement, etc. decision-makers) because they highlight the background, causal links, and effects of the events that have occurred so far (in this case, terrorist attacks). By contrast, conclusions may also include a list of possible consequences and some kind of forecast. The production of forecasts is one of the main tasks of the analytical/evaluation organisation because it is the best way to support users *(Vida 2013: 90)*.

Participation of special police units in counter-terrorism work

From the outset, commandos were used mainly for military operations requiring a small but specially trained and equipped unit that could be deployed very quickly. This capability is particularly important when one considers one of the greatest security challenges of the recent past and present, terrorism. However, the military solutions used to prevent and disrupt (eradicate) terrorist attacks in non-war areas have proved less effective and, as seen above, raise various legal concerns. Related to this is the fact that most nation-states strictly regulate or even prohibit the deployment of their armies within their borders in peacetime. This legal situation, together with the terrorist attacks in Europe in the 1970s, led to the creation of special police units trained and equipped to combat terrorism. From this point of view, terrorists are criminals and, in accordance with all democratic standards of the rule of law, it is the task of the police to detect, apprehend, investigate and prosecute them. It is the duty of the judicial authorities to prosecute, try and punish them *(Rada–Vajda 2010: 150)*.

Rapid reaction teams with special weapons and tactical procedures have therefore been set up in the police field to apprehend terrorists and prevent and eradicate terrorist acts. The most familiar and perhaps most apt acronym for these units is the American acronym SWAT (Special Weapons and Tactics). Names vary from nation to nation, and it is even the case that parallel groups within a nation are given different names. Examples are the GIGN (Groupe d'intervention de la Gendarmerie nationale – National Gendarmerie Intervention Group) and the special police unit RAID (Recherche, Assistance, Intervention, Dissuasion – Research, Assistance, Intervention, Deterrence) in France, the GSG9 (Grenzschutzgruppe 9

– Border Protection Group 9) in Germany, which has federal jurisdiction, and the SEK (Spezialeinsatzkommando – Special Task Force) and MEK (Mobile Einsatzkommandos – Mobile Task Forces), which operate on a regional basis. As you can see, virtually all special police units have one of the above-mentioned terms in their names, namely rapid reaction, tactical, and intervention. To summarise, we are talking about small, rapidly mobilisable tactical units with specially trained personnel, equipped with special weapons and techniques, whose primary task is to carry out unexpected special law enforcement operations *(Kasznár 2017: 353)*.

Conclusion

In this paper, I have developed and presented a kind of general, logical-functional counter-terrorism model for the specific, complex activities of counter-terrorism services, based on my own ideas, studies, and professional experience, which has not been developed in such a complex form so far, albeit sketchily. It has been shown that terrorism is fundamentally a highly dynamic illegal activity and that countering or countering it, therefore, requires primarily dynamic tools and methods on the part of the counter-terrorism services. The theoretical model that I have developed and present here has been used to briefly describe these tools and methods. Based on my many years of professional experience, it can be said that no single tool or method is sufficient in itself to combat terrorism effectively. Only the combined or complementary application of the methods presented in this study can lead to results.

I have clarified the distinction between defensive and offensive counter-terrorism. According to the theoretical framework I have set out, it is the socio-political context and the objective to be achieved that essentially determines the basis for the definition of defensive or offensive counter-terrorism. However, counter-terrorist action must not go beyond the use of devices and methods that are permissible in the rule of law. I am thinking here of the fact that the rule of law principles of counter-terrorism, respect for necessity, and proportionality, cannot limit the extent of covert interventions, even because of the scale of the threat. Therefore, on the one hand, I believe that it is a mistake to define the fight against terrorism as a war, and on the other hand, I believe that a distinction must be made between military and law enforcement methods in counter-terrorism.

The study will be complemented by a discussion of the main counter-terrorism tasks of the police, and more specifically the specific element of the police's role, namely the eradication of terrorist acts. Operational/enforcement forces, and here we are talking primarily about law enforcement forces, must be prepared to develop rapid and effective procedures to carry out the specific tasks assigned to them professionally and safely. In all cases, the tactical procedures must also be in accordance with the legal provisions in the given State and the tactical principles for their application.

References

Boda J., & Regényi K. (2019) A hírszerzés története az ókortól napjainking [The history of intelligence from Antiquity to the present day]. Budapest, Dialóg Campus Kiadó.

Dávid F. (2018) Történeti visszatekintés a magyar titkosszolgálatokra [Historical review of the Hungarian secret services]. In: Resperger I. (ed.) A nemztebiztonság elmélete a közszolgálatban [Theory of national security in the civil service]. Budapest, Campus Dialóg Kiadó. pp. 15–32.

Dobák I. (2018) Az információgyújtésről általában [On information gathering in general]. In: Resperger I. (ed.) A nemzetbiztonság elmélete a közszolgálatban [Theory of national security in the civil service]. Budapest, Campus Dialóg Kiadó pp. 74–83.

Dobák I. (2017 June) Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében [Technical information gathering in the light of changing security challenges]. Hadmérnök, Vol. XII. No. 2. pp. 235–249. http://hadmernok.hu/172_19_dobak.pdf [Downloaded: 14 Jan 2022].

Finszter G. (2002) Az alkotmányos jogállam esélyei a terrorizmus elleni küzdelemben [The chances of the constitutional rule of law in the fight against terrorism]. Belügyi Szemle, Vol. 51. No. 6–7. pp. 156–166.

Hautzinger Z. (2006) Büntetőeljárás a terrorizmus árnyékában. A Katonai Biztonsági Hivatal Tudományos Tanácsának Kiadványa – Szakmai Szemle, 2006. 2. szám. [Criminal procedure in the shadow of terrorism. Szakmai Szemle, publication of the Scientific Council of the Military Security Office, issue 2], pp. 33–43.

Kasznár A. (2017) Bevezetés a terrorelhárítás alapjaiba [Introduction to the basics of counter-terrorism]. Budapest, Dialóg Campus Kiadó. pp. 353–355.

Kőszegvári T. (2002) A nemzetközi terrorizmus elleni harc katonai területei és feladatai. (Egyetemi jegyzet, ZMNE Budapest, 2003.) [Military tasks in the fight against international terrorism.] http://www.zmne.hu/kulso/mhtt/hadtudomany/2002/1/z-01/chapter1.html [Downloaded: 10 Mar 2019].

Maras, M-H. (2016) The theory and practice of terrorism. Antall József Knowledge Center.

Nagy K., & Mezei J. (2020) Nemzetközi kitekintés a terrorelhárítás területén folytatott biztonságtudatosítási programokba [International perspective on security awareness programmes in the field of counter-terrorism]. Nemzetbiztonsági Szemle, Vol. 8, No. 2, pp. 50–65. http://real.mtak.hu/118095/1/WEB---NSZ_2020_2-4_NagyKMezei_50-65.pdf [Downloaded: 12 Dec 2021].

Rada M., & Vajda V. (2010) A terrorizmus elleni küzdelem, avagy a 22-es csapdája [The fight against terrorism, or the Catch-22]. Külügyi Szemle, Spring issue. pp. 139–170. https://kki.hu/assets/upload/Kulugyi_Szemle_2010_01_A_terrorizmus_elleni_kezd.pdf [Downloaded: 21 Oct 2020].

Vida C. Dr. (2013) A hírszerző elemző-értékelő munka alapjai [The basics of intelligence analysis and assessment]. Felderítő Szemle, Vol. XII. No. 3. pp. 90. http://real.mtak.hu/14875/13/jav_real__2013-3.pdf [Downloaded: 12 Jan 2022].

Weimann, G. (2004) www.terror.net Gabriel Gabriel: How modern terrorism uses the internet. Washington D.C. United States Institute of Peace, pp. 5–10. https://www.usip.org/sites/default/files/sr116.pdf [Downloaded: 10 Dec 2021].