VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 20
no. 2
pp. 163–181

Comparing Counterintelligence and Counterterrorism – Similarities, Issues and Solutions

Jaroš Britovšek

Purpose:

This paper aims to discuss and compare counterintelligence and counterterrorism, particularly in the aftermath of the Cold War and the rise of new forms of non-state terrorism, and critically examine the tendency of western liberal democracies to assign counterterrorism tasks to services traditionally involved in counterintelligence. The aim is therefore to identify similarities, differences and issues that arise between these two activities. In addition, some solutions to the issues presented are proposed.

Methods:

Models and concepts are developed and presented through analysis of primary and secondary sources. Several aspects are identified, leading to a comparative analysis being conducted.

Findings:

Counterintelligence and counterterrorism seem very similar at first glance, but differ from each other in certain important respects. They both lie on a spectrum between a 'law enforcement model' and an 'intelligence model', and can overlap when targeting state-sponsored terrorism or state and non-state actors' intelligence activities. Yet they vary substantially when dealing with risks, time sensitivity and the sharing of information, and ignoring them can have a significant impact on national security.

Research Limitations:

Besides the secret nature of intelligence and, therefore, limited access to information, the paper primarily focuses only on states' security apparatus and does not consider other political, societal or psychological actors or approaches.

Practical Implications:

In the paper, several solutions derived from the principle of the separation of counterintelligence and counterterrorism are presented for policymakers, while also calling for the establishing of sharing and coordination bodies.

Value:

This paper counters the prevailing paradigm that overemphasises the role of the traditional services involved in counterintelligence as part of the fight against modern terrorism. The findings and conclusions are intended for political, professional and wider public audiences.

UDC: 351.746.1:343.3

Keywords: counterintelligence, counterterrorism, intelligence and security services, law enforcement

Primerjava protiobveščevalne in protiteroristične dejavnosti – podobnosti, dileme in rešitve

Namen prispevka:

Namen prispevka je obravnavati ter primerjati protiobveščevalne in protiteroristične dejavnosti, še posebej z vidika konca hladne vojne in pojava novih oblik terorizma, ter kritično obravnavati nagnjenja zahodnih liberalnih demokracij, ki vlogo protiteroristične dejavnosti potiskajo v organizacije, ki so bile tradicionalno zadolžene za protiobveščevalno dejavnost. Cilj je torej predstaviti podobnosti, razlike ter dileme. Glede na identificirane dileme so predstavljene tudi nekatere rešitve.

Metode:

Za razvoj modelov in konceptov je bila uporabljena analiza primarnih in sekundarnih virov. Identificiranih je bilo več vidikov, na podlagi katerih je bila nato opravljena primerjalna analiza.

Ugotovitve:

Protiobveščevalna in protiteroristična dejavnost se zdita na prvi pogled podobni, vendar obstajajo med njima pomembne razlike. Obe ležita na spektru med 'modelom organov pregona' in 'obveščevalnim modelom' ter se na nekaterih področjih tudi prekrivata, kot je spremljanje državno-sponzoriranega terorizma ter terorističnih skupin, ki uporabljajo obveščevalno dejavnost. Dejavnosti se razlikujeta predvsem na področju tveganj, časovne občutljivosti ter uporabe informacij. Neupoštevanje teh razlik ima lahko pomembne posledice za nacionalno varnost.

Omejitve:

Poleg tajne narave obveščevalne dejavnosti in s tem omejenega dostopa do informacij se prispevek osredotoča predvsem na varnostni aparat države in se hkrati izogiba ostalim političnim, družbenim ter psihološkim akterjem in pristopom k tematiki.

Praktična uporabnost:

V prispevku je predstavljenih več rešitev za odločevalce, ki izhajajo iz načela delitve protiobveščevalne in protiteroristične funkcije. Izražena je tudi potreba po centru, ki bi omogočal koordinacijo in izmenjavo informacij.

Izvirnost/pomembnost prispevka:

Prispevek nasprotuje prevladujoči paradigmi, ki daje pretirano vlogo v boju proti modernemu terorizmu službam, ki so tradicionalno vpete v protiobveščevalno delo. Ugotovitve so namenjene politični, strokovni in širši javnosti.

UDK: 351.746.1:343.3

Ključne besede: protiobveščevalna dejavnost, protiteroristična dejavnost, obveščevalne in varnostne službe, organi pregona

1 INTRODUCTION

Counterintelligence and counterterrorism are both significant activities of any national security system, with each serving their particular purpose and goals. While authors are chiefly concerned with either counterintelligence (Podbregar & Ivanuša; 2016; Prunckun, 2012, 2014; Van Cleave, 2013) or counterterrorism (Crelinstein, 2014; Pedahzur, 2009), some (Gleghorn, 2003; Mobley, 2012) also promote the use of counterintelligence tradecraft against terrorism. Following the Cold War and the rise of new forms of threats such as non-state sponsored terrorism, the tendency of western liberal democracies has been to assign counterterrorism tasks and responsibilities to intelligence and security services traditionally involved in counterintelligence (Bauer, 2016). Although counterintelligence and counterterrorism sometimes overlap, confusing them may have a significant impact on national security as they essentially differ in their nature, purpose and goals. Both activities aim to neutralise specific threats. By definition, counterintelligence deals with countering a foreign intelligence threat, while counterterrorism deals with preventing a terrorist threat. Intelligence and terrorism are defined in a multitude of ways, with no firm consensus of what each constitutes (Warner, 2002; Weinberg, Pedahzur, & Hirsch-Hoefler, 2004).

Intelligence itself is an elusive concept, but at its core it is concerned with data and information. It consists of three fundamental elements: the collection of data and information, analysis of collected data and information, and counterintelligence, or preventing an adversary from collecting data and information about oneself. Counterintelligence is a vital activity for protecting secrets. It is therefore pitted against other entities' intelligence activities and usually also an integral part of a state's intelligence efforts (Britovšek, Sotlar, & Tičar, 2017). However, intelligence services are not only involved in intelligence gathering. Warner (2002, p. 21) defined intelligence as a "secret, state activity to understand or influence foreign entities", meaning that besides espionage some states use intelligence agencies to conduct covert action or special measures in order to influence other political entities. Counterintelligence therefore also includes countering activities of influence (covert actions), such as subversion, sabotage and even terrorism[1] (Van Cleave, 2013).

1 *Counterintelligence tasks can also include counterpropaganda or countering 'fake news', to use a more fashionable term, or protecting a country's electoral process. Russian intelligence and propaganda interference in the 2016 presidential election in the United States is a recent example of this (Priest, 2017).*

In contrast, terrorism is difficult to define due to different, often opposing political interests, and to date there is no universally objective and internationally accepted definition of terrorism (Ramsay, 2015; Richards, 2014; Schmid, 2004). One reason for this, at least according to Bauer (2016), is that "nothing more resembles a terrorist than a resistance fighter". Yet some efforts have been made to identify certain key elements of terrorism that go some way to defining it. To distinguish it from other criminal acts, Hoffman (2006, p. 40) defined terrorism "as the deliberate creation and exploitation of fear through violence or the threat of violence in pursuit of political change". In addition, Weinberg et al. (2004, p. 782) stated that "terrorism is a politically motivated tactic involving the threat or use of force or violence in which the pursuit of publicity plays a significant role". Counterterrorism's main role is therefore to counter politically motivated illegal acts of violence.

Countries differ in their approaches to national security issues, which in turn depends significantly on how they perceive the threats they face. Intelligence tends to be divided into foreign intelligence and security intelligence. The former focuses on foreign governments and situations external to the service's home country, while the latter focus, but are not necessarily limited to, domestic or internal security threats (Herman, 1996). They are further divided into military and civilian counterparts. However, due to the hybridisation and overlapping nature of security threats in the contemporary international order, the lines between foreign and domestic, military and civilian, have been blurred considerably (Britovšek & Čretnik, 2016). Here, the differences between counterintelligence and counterterrorism may be explained and compared through two models of addressing the threats each is intended to neutralise: a 'law enforcement model' and an 'intelligence model'.

2 LAW ENFORCEMENT AND INTELLIGENCE MODELS

To better understand the frameworks and concepts according to which counterintelligence and counterterrorism operate, two models[2] have been developed to allow a more coherent analysis and comparison of the two activities; a 'law enforcement model' and an 'intelligence model' (see the simplified comparison of these models in Table 1). The 'law enforcement model' derives and is based on the legal feature or public law, while the 'intelligence model' originates and is based on political considerations, partly diplomatic and partly military, depending on the situation of a particular country. The models lie on a spectrum ranging from legal towards more political and military aspects, which will help us understand the issues and differences arising from counterintelligence and counterterrorism, and will also locate both activities on the spectrum these two models lie on.

2 *The models have been derived, modified and adapted from already developed coercive models with regard to counterterrorism: the 'criminal justice model' and the 'war model'. The 'criminal justice model' perceives terrorism as a criminal act, using police to deal with it within the criminal justice system's restraints, while the 'war model' perceives terrorism as part of war, as revolutionary warfare, consequently using also hard force such as military action to eliminate or defeat terrorist threats (Crelinsten, 2014).*

The 'law enforcement model' presupposes a more stable operating environment of the 'rule of law', whereas the 'intelligence model' works in a more competitive, chaotic and hostile environment that is less constrained by a transparent framework or laws, rules and regulations. The main aspects of both models have been identified and compared and, with the support of each, counterintelligence and counterterrorism have been further compared and analysed with regard to several identified issues. The overlap and most significant differences have been identified and explained, leading to the conclusion that counterintelligence and counterterrorism should not be conflated, or perhaps even be conducted by the same organisational or institutional structures.

Table 1: Comparison of the 'law enforcement model' and 'intelligence model' in the context of counterintelligence and counterterrorism

	Law enforcement model	**Intelligence model**
Main aspect	Perceiving and treating terrorism, espionage, subversion and sabotage as criminal acts	Perceiving and treating terrorism as a political or war tactic and intelligence as an auxiliary element of one's opponent
Environment	Legal environment with an emphasis on the rule of law	Competitive political environment, which in extreme cases can lead to war
Means and aim	To investigate, arrest and prosecute according to the rule of law	To gather and analyse intelligence on one's opponents' capabilities and intentions
Agents	Police and criminal justice system	Intelligence and security services
Information	Gathering evidence to be legally used in courts	Gathering intelligence with an emphasis on secrecy
Issues	Punishment not enough to deter politically motivated culprits Lack of knowledge before crimes are committed	Overemphasis and expansion of surveillance (delay of action) Ignoring or violating of basic human rights
Benefits	Delegitimises culprits as mere criminals	Preparation and possible prevention of threats

The models differ in several respects. These can be explained by their roots in different organisational cultures: one originating in law enforcement and the other from intelligence services (Hulnick, 1997). Starting with the main aspect, the 'law enforcement model' perceives terrorism as well as some intelligence activities such as espionage, sabotage and subversion as criminal acts, while the 'intelligence model' considers terrorism a political or military tactic and intelligence as an auxiliary element of an opponent's effort to achieve political or military goals. The 'law enforcement model' also assumes a stable legal framework and responds to criminal acts in compliance with the law and is subjected to constant judicial oversight. The means and aims are investigations, arrests and prosecutions according to the rule of law. Its primary agents are police agencies and the broader criminal justice system. The model perceives the world in a black-and-white manner of legal and illegal, while the 'intelligence model' sees the world more in shades of ambiguous grey (Gleghorn, 2003).

The 'intelligence model' functions in the more politically competitive international environment, which can – following Clausewitz's principles – in certain circumstances and extreme cases develop into war. The means and aims of the 'intelligence model' concentrate on gathering and analysing intelligence

on one's opponents, assessing their capabilities and trying to understand their intentions (Vandepeer, 2011). Consequently, these activities are by nature much slower and more time-consuming than law enforcement investigations (Gleghorn, 2003). The main agents are intelligence services, or perhaps to be more precise in the context of counterintelligence and counterterrorism, security services. The latter depends on the countries' organisational framework; separated or combined foreign and security intelligence for example.

An important point of the distinction between the two models is the role of information in either's activities. The 'law enforcement model' focuses on gathering and establishing evidence, while the 'intelligence model' gathers data and information with the aim to produce intelligence reports for decision-makers regarding opponents' capabilities, plans and intentions. Information in the 'law enforcement model' refers to evidence, which has to satisfy specific legal standards or burdens of proof, such as 'probable cause' and 'beyond a reasonable doubt'. Its core objective is to prove that someone is guilty of a crime or not. On the other hand, information in the 'intelligence model' refers to intelligence, with a lower evidentiary standard and greater emphasis on assessments and prognosis. The latter derives from working in a more uncertain environment, trying to gain access to opponents' secrets, reveal their intent, and where they will likely try to counter one's own intelligence efforts. The main objective in the latter model is not to prove guilt as in the former, but to inform policymakers or military leaders (Berkowitz, 2003).

Both models have their advantages and disadvantages. In the 'intelligence model', the state receives intelligence reports on the current situation and possible future threats to form a clearer understanding of the opponent and, thus, take preventative actions by applying appropriate measures. But the nature of intelligence work makes agencies prone to the over classification of their products which are primarily meant for decision-makers, thus rendering it difficult to share with other relevant agencies (Goitein & Shapiro, 2011). The lower evidentiary standard and secrecy make it difficult to use intelligence (information) in courts and criminal justice proceedings (Bigo, Carrera, Hernanz, & Scherrer, 2015; Eijkman & van Ginkel, 2011). Moreover, overemphasising the role of intelligence can not only lead to overproduction and lack of action (Lutwak, 2015), but also to increased surveillance of ordinary citizens, which consequently risks ignoring basic human rights, especially without proper and effective oversight mechanisms (Lubin, 2017).

Conversely, the 'law enforcement model' follows a more legalistic and thus more legitimate process, utilising the 'rule of law' when dealing with suspects. Even if there was a political agenda, treating it as a mere crime can also have a delegitimising effect on the culprits' political ideology and goals. A deficiency of the model is too much emphasis and reliance on punishment, thus missing the point that highly politically motivated persons will not be deterred by the mere fear of punishment (Crelinsten, 2014). This reliance and focus on punishment risks law enforcement agencies becoming wilfully blind to any events occurring before a crime is prepared or carried out, thereby hindering the prevention of incidents (Treverton, 2009).

3 COUNTERINTELLIGENCE AND COUNTERTERRORISM

Counterintelligence and counterterrorism do not fall strictly into one model or the other. They usually lie on a spectrum between the 'intelligence model' and the 'law enforcement model', which depends on a state's institutions, organisations, history, culture and legislation. In general, counterintelligence lies closer to the 'intelligence model', working in a more politically competitive environment, while counterterrorism lies closer but is not strictly confined to the 'law enforcement model', with its greater emphasis on the legal framework and its attending constraints.

There is a reason the tasks of counterintelligence and counterterrorism are often perceived as being very similar, as they do overlap on some issues. This is especially seen in the 'intelligence model' because they both use surveillance techniques when monitoring their targets. Another common feature is the role of intelligence analysis, especially in risk[3] assessment, or assessing one's own vulnerabilities and identifying potential threats (Crelinsten, 2014; Prunckun, 2012; Vandepeer, 2011). In the 'law enforcement model', there is an overlap when criminal investigation is involved as both terrorism and some intelligence activities like espionage are considered criminal acts. Consequently, gathered information must fulfil certain evidentiary standards to allow its lawful and effective use in courts.

Another overlap between counterintelligence and counterterrorism are the threats themselves. On the one hand, states can be involved or otherwise support non-state groups that conduct terrorist acts. On the other, non-state groups, otherwise involved in terrorist attacks, can use intelligence gathering and espionage to support their main activities[4]. The interplay between states and non-state groups, as well as the rise of non-state groups' intelligence capabilities, is an area where counterintelligence and counterterrorism meet and cooperate. In order to enhance such cooperation, coordination and also the de-confliction of activities, states can and should establish coordination and information centres for these purposes (Britovšek & Čretnik, 2016).

Counterintelligence and counterterrorism are also dissimilar in their activities and functions, meaning there are significant differences when comparing the two activities on different organisational levels. Counterterrorism is a more independent activity, concentrating more or less on the obvious threat of terrorism, while counterintelligence is as an auxiliary element to other activities and depends on the organisation that employs it, that is, elements of counterintelligence can be used to protect the confidentiality of information, operations and sources in the police, intelligence, military or private sector (Britovšek et al., 2017; Prunckun, 2012). This difference means that counterintelligence can be more readily applied in the course of counterterrorism activities than vice versa.

3 *As I explain later, imminent risks are more a feature in counterterrorism, where it is essential that intelligence analysis 'gets it right', connecting the right dots at the right time and finding the right targets (Bauer, 2016).*

4 *For example, Hezbollah, a Shiite militant group from Lebanon with strong links to and support from Iranian intelligence, has been known to be involved in terrorist attacks (Azani, 2013). But through the years Hezbollah was also able to develop its own military and intelligence capabilities (Harber, 2009).*

Due to historical reasons and institutional evolution, the tasks of counterterrorism were pushed into the hands of agencies that knew how to conduct counterintelligence, but not how to counter the new forms of terrorism emerging after the Cold War. Terrorism during the Cold War was essentially part of the struggle between the two main antagonistic powers: the United States and the Soviet Union. Terrorist groups were active but were supported, managed or tolerated by the opposing states and their intelligence services (Bauer, 2016). Their biggest targets were foreign states and their intelligence services. The main reason counterintelligence played a major role in combating terrorism was due to this link to states as sponsors and targets. But the primary targets were always foreign intelligence activities. When communism/socialism collapsed, politically left-leaning terrorist groups practically disappeared[5]. The key point here is that countering terrorism was understood to be a function of and managed by states' intelligence services.

But as the environment changes and evolves, so does the threat. After the collapse of communism, the greatest threat, the Soviet Union and its allies, disappeared and western intelligence and security services started losing their *raison d'être*. From a historical point of view, intelligence and counterintelligence usually rise to prominence when there is a highly competitive or hostile environment, usually between religious, national or ideological blocs or coalitions. Such were the periods of the religious wars between Catholics and Protestants in Europe and the ideological rivalry between the United States and the Soviet Union during the Cold War (Liulevicius, 2011). The 'intelligence model' thrives in competitive environments. Yet, after the collapse of communism, the level of hostilities and competition fell drastically, and with it the foreign intelligence threat and the importance of counterintelligence[6].

However, the rise of non-state, Islamist extremism and terrorism, and the re-emergence of intelligence threats from countries such as Russia and China, returned the focus to intelligence and security services. The problem is that the task of counterterrorism has been assigned to agencies that were responsible for either counterintelligence or law enforcement. Bauer (2016) argues that most western counterterrorism activities are today being conducted by agencies that traditionally worked in the field of counterintelligence, as that was the purpose for their establishment. States did not properly recognise the cultural evolution of terrorism, which transitioned to the "hybridization of criminality, religious fanaticism, and terrorism". The need to understand this difference is therefore essential for providing possible organisational solutions to issues concerning counterintelligence and counterterrorism.

Counterintelligence and counterterrorism have both common and distinguishing features which can be recognised through the lenses of either the

5 *For example, the German left extremist group 'Baader-Meinhof' announced its disbandment in 1998, which was five years after its last terrorist attack (Lockwood, 2011).*

6 *For example, legislators in the United States drastically cut the intelligence budget in the aftermath of the fall of communism. The number of personnel employed in the intelligence community dropped by about a sixth in the mid-1990s. Similarly, in the United Kingdom, intelligence and security services faced lower budgets and the first personnel layoffs since World War II (Warner, 2014).*

'law enforcement model' or the 'intelligence model'. Through further analysis, we attempt to prove that although several aspects of counterintelligence and counterterrorism are similar, there are significant differences which can have a serious impact on the overall efficiency of national security (for the purpose of this analysis, see the simplified version of the counterintelligence and counterterrorism comparison in Table 2). As mentioned, the main aim of counterintelligence is to counter the intelligence threat, while the main aim of counterterrorism is to counter the terrorist threat. The intelligence threat usually comes from foreign states and their intelligence services, while the terrorist threat often comes from international terrorist organisations and domestic political extremist groups or individuals.

Table 2: Comparing counterintelligence and counterterrorism

	Counterintelligence	**Counterterrorism**
Aim and focus	To counter the intelligence threat To protect institutions (state and non-state)	To counter the terrorist threat To protect institutions and the civilian population
Threat	Foreign states	Domestic and/or foreign political extremists
Defensive role	Protecting secrets Deterrence and detection	Protecting potential targets and victims Target hardening Critical infrastructure protection Monitoring people, money, goods and services
Proactive role	Detection, deception and neutralisation	Detection, disruption, prevention and neutralisation
Imminent risks	Loss of information	Loss of life
Time	Ally (long-term investigations tolerated)	Enemy (urgent short-term action)
Information	Need to know	Need to share
Overlap	Risk assessments and surveillance Evidentiary standard and prosecution State-sponsored terrorism Non-state group intelligence efforts	

3.1 The Defensive Role of Counterintelligence and Counterterrorism

Counterintelligence and counterterrorism can be divided into defensive and proactive[7] roles. Pedahzur (2009) added a defensive model to the other counterterrorism models mentioned earlier. The defensive model does not deal directly with potential terrorists but focuses on the protection of potential targets and victims of terrorism. The same can be applied to counterintelligence, with

7 *Counterintelligence and counterterrorism are usually divided along defensive/offensive or passive/active modes or lines (Duvenage & Von Solms, 2015). But because these roles are not easily distinguishable from each other, and often overlap, we use a somewhat hybrid distinction, using defensive and proactive modes as a benchmark.*

the exception that its chief mission is to protect state secrets (Britovšek, 2017). Defensive counterintelligence includes deterrence and detection (Prunckun, 2012, 2014), while defensive counterterrorism encompasses target hardening, protection of critical infrastructure and the monitoring and regulation of the flow of people, money, goods and services (Crelinsten, 2014). All of these defensive activities strive to deny or discourage opponents' activities. However, some measures will differ since deterring mere access to information, usually held in a government facility or computer network, is not the same as hardening a target from a kinetic attack whose aim is to kill or cause as much physical damage as possible to facilities, infrastructure and civilian population.

Defensive counterterrorism's role is not strictly or exclusively reserved for law enforcement and security services. Because the terrorist threat endangers a much wider population, counterterrorism is usually implemented throughout national security structures (e.g. military, police, border controls and immigration officers) including the private sector (e.g. private security and banking system) (Crelinsten, 2014). On the other hand, defensive counterintelligence is more limited and concentrated on protecting certain organisations or institutions. It is manifested in physical security, personnel security (vetting), information security and communications security of the organisation it seeks to protect (Prunckun, 2012).

3.2 Proactive Roles of Counterintelligence and Counterterrorism

Both counterintelligence and counterterrorism have proactive roles. The starting point of proactive counterintelligence is detection, which may also be considered part of its defensive role. It is an act of noticing an event that is or can be associated with a breach or potential breach of secret or protected information. This leads to an investigation and surveillance of the targets (Prunckun, 2012). The agency then has a choice regarding how to neutralise the threat. This depends significantly on the abovementioned environment. It can decide to follow the 'law enforcement model' and gather evidence and prosecute the culprits, or use the 'intelligence model' and gather more intelligence and find out more about the *modus operandi* of those responsible, also utilising deception techniques to neutralise the threat. The gathered information is used in threat and risk assessments according to which the agency and the state can implement new defensive measures to further deter the threat.

Although counterintelligence also deals with certain crimes such as espionage, subversion and sabotage, it is rare for counterintelligence cases to be brought before the court in criminal proceedings. The focus is more on observing, exploiting and managing the threat than prosecuting the culprits. In most cases, the responsible agents are members of a foreign state intelligence service, often with diplomatic immunity, and prosecuting them would rarely bring the desired results. What is more certain is that any action against state agents, like naming certain individuals *persona non grata*, will be followed by similar steps from the opposing state. So-called 'tit for tat' retaliation or reciprocity is one of the main mechanisms that regulates and manages the behaviour of most countries and their

diplomatic personnel in the international environment (Fakhoury, 2017). States' leadership must therefore often act wisely when foreign agents are discovered or need to assess their countries' global position, their international relations or economic and political interests.

In some respects, counterintelligence can be viewed similarly to investigations dealing with organised crime. Professionals will traditionally work backwards, from a crime or event up the operational chain, covertly mapping the organised networks and slowly building a case against them. To further illustrate, investigations of an organised criminal group or foreign intelligence service depend on surveillance of several transfers of illicit goods or 'stolen' sensitive information. The research is built slowly, gathering all the intelligence and, in the case of organised crime, also collecting relevant evidence that must meet the judicial system's evidentiary threshold. It would make no sense to use the same techniques in counterterrorism where the equivalent to a one-off drug shipment or stolen secret would be a single terrorist attack. But the whole aim of counterterrorism is to prevent that one attack, which should make it obvious that counterterrorism differs from counterintelligence and organised crime investigations. The key point here is that time can be an ally in counterintelligence. Yet this is not the case with counterterrorism, where the exact opposite is true. Time is an enemy and delaying action can prove fatal (Bauer, 2016).

Issues and rivalries also arise from different cultures within the police on one hand and intelligence and security services on the other. The role of intelligence is to collect and analyse intelligence, while the role of the police is to investigate and prevent crimes through prosecution. The former makes sense when dealing with foreign intelligence but not when a terrorist act is being planned or conducted, as the case of a German neo-Nazi group demonstrates[8]. The latter needs urgent interference and disruption, not time-consuming intelligence gathering and mapping of a whole network while lives are at stake. Bringing suspects in, questioning them and conducting thorough investigations may be more effective and could save lives.

According to Lutwak (2015), it all comes down to the question of methods, derived from one fundamental insight: "Terrorist actions cannot be anticipated and prevented – all such efforts are simply futile because there are just too many possible targets and infinity of possible dates. Nor can one hope to detect even imminent attacks because terrorists need not reveal themselves until it is too late". Surveillance of all suspects, who in some countries can be quite numerous[9], is practically impossible as that would take up a significant number of personnel and resources. Further, the most intrusive surveillance methods in western liberal

8 *For example, from 2000 to 2007 Germany witnessed a series of murders of migrants committed by a neo-Nazi group. Germany's security service had the group under surveillance. However, members of the group were able to conduct ten murders in the period when the service had paid informants who were also close to the perpetrators. The agency had known the leading culprits and their organisation had been known to them since the early 1990s, but they failed to share information with the police, who were investigating these crimes. Besides institutional failure in sharing information, there is also the issue of rivalry between the intelligence and security services and the police (McGowan, 2014).*

9 *For example, according to French authorities in 2016 around 20,000 people represented a security risk in France (Peter, 2016).*

democracies are usually legally restrained in scope and duration. In the case of counterterrorism, the solution is to bring down the number of relevant suspects to a manageable size, and taking action the moment the first indications of potential involvement in terrorism come to light, as is the case with Italy[10]. The issue is that most European countries' intelligence and security services have included counterterrorism in their intelligence and counterintelligence framework (Bauer, 2016) where they tend to prolong the surveillance of suspects and write multiple reports and assessments for policymakers. This is appropriate for pure intelligence work, somewhat less so for counterintelligence, and not at all for counterterrorism.

3.3 Risks, Time Sensitivity and Sharing of Information

There is a large qualitative gap between the risks pertaining to unsuccessful counterintelligence and counterterrorism efforts. In the case of counterintelligence, the primary imminent risk is the loss of information, meaning sensitive information or secrets that enable a state to function or stay ahead of other states, especially hostile ones. This risk varies regarding the level of competition and hostility in the environment (Britovšek, 2017). On the other hand, failure in counterterrorism holds imminent risks for lives and property. Loss of information can in some cases lead to the loss of life but usually in the context of a war or as an indirect consequence. There are, however, considerably fewer traumas compared to terrorism where there may be a direct loss of lives, especially civilians'. The latter can trigger drastic changes in policy as seen in the examples of increased surveillance and wars in Afghanistan and Iraq (Adams, Nordhaus, & Shellenberger, 2011), while failure to protect secrets, although damaging, typically does not have the same drastic impact on policy.

The need to act upon threats is therefore more urgent in counterterrorism than in counterintelligence because there is exposure to a greater imminent risk, namely the loss of lives. Consequently, to ensure proactive counterterrorism it is essential to fuse the 'law enforcement model' and 'intelligence model' by for example identifying dangerous people, profiling, surveillance, intelligence-led policing, sting operations and preventative detention (Crelinsten, 2014). Urgency also brings forward the 'need to share' principle in counterterrorism, which lies in contrast to counterintelligence dealing with foreign governments where secrecy is of the outmost importance and where the 'need to know' principle prevails.

There is a constant conflict between the need to balance the 'need to know' and 'need to share' principles in information-oriented organisations. The former notion is associated with who gains access to sensitive information and who does not. This essentially means ensuring that the right person has access to and insight

10 *In most cases, a friend or an acquaintance would report a person that is bragging or speaking of carrying out or supporting violent attacks. What follows such a report is a thorough interrogation and investigation that reveal if there is any more to the initial indication. If a suspect's militancy is confirmed, they are held while investigators check additional records to build a criminal case as part of which they could arrest, try and imprison the suspect (Lutwak, 2015). Italy has also relied heavily on administrative measures. Thus far, one of the most successful counterterrorism measures, at least in the short to medium term, has been the deportation of foreign suspects in association with restrictive naturalisation laws (Marone, 2017).*

into certain information, which they need to perform their duties, and limited or no access to information they do not require (Best, 2011). This 'need to know' principle applies especially to counterintelligence since the protection of sensitive information is one of its crucial goals. The value of that principle rises along with the environment's level of competitiveness. The 'need to share' principle became prominent after the 9/11 terrorist attacks in the United States. The investigation of the handling of the attack found that 'stovepiping' and bureaucratic hoarding of information had contributed to a major counterterrorism failure (Miller, 2011).

However, the sharing of information also creates possibilities for leaks, which is a main concern of counterintelligence, particularly in the context of relations with other states. Counterterrorism, in dealing with protecting people's lives, unlike counterintelligence (which deals with protecting information), needs prompt, actionable and useable information. If both activities are conducted by the same organisation, tensions between these principles will arise which, if unresolved, can have a paralysing effect on a state's overall national security (Bauer, 2016; Miller, 2011). In addition, besides the mentioned lower evidentiary standards of intelligence, the 'need to know' principle leads to secrecy and the use of secret intelligence in courts can threaten the fairness of legal proceedings and make it more difficult to conduct prosecutions or hold governments accountable for misconduct (Roach, 2015).

4 OVERCOMING THE ISSUES AND PROPOSED SOLUTIONS

Considering the abovementioned differences and conflicts between counterintelligence and counterterrorism, issues emerge by virtue of most western countries assigning the tasks of counterterrorism to their agencies that have traditionally been involved in counterintelligence. To deal with these issues, we devised four principles to be considered while locating counterintelligence and counterterrorism within the organisational or institutional structure of a national security system. First, the 'intelligence model' is needed for identifying threats and assessing risks. Second, the 'law enforcement model' is needed for lawfully disrupting and prosecuting suspects. Third, the 'need to share' principle is essential in counterterrorism, while the 'need to know' principle is vital for counterintelligence. Finally, time is immensely important for counterterrorism, but less important in counterintelligence.

In accordance with these principles, some organisational solutions are presented. When dealing with organisational and institutional issues, we propose the separation of counterintelligence and counterterrorism at the state level; leaving counterintelligence as part of the traditional security and intelligence structures and establishing a new agency to take the lead in and work exclusively on counterterrorism issues. The burden and constraints of counterintelligence at the state level would be lifted from this agency, meaning it could share information rapidly and freely, while counterintelligence would continue to focus on protecting sensitive information in relation to foreign intelligence threats. In the context of counterterrorism, the application of counterintelligence can then be applied as needed, usually with a limited scope, such as the operational security of ongoing investigations.

There is also an option to reform the current institutional structures. As most states have separate defence and interior ministries, it would be economical and sensible to separate responsibilities between these ministries, especially in smaller states. The ministry responsible for defence is responsible for defending the state from foreign threats, mainly foreign governments, their institutions and activities. It therefore makes sense to place state counterintelligence tasks with the defence ministry, or its security intelligence department. The tasks of counterterrorism would be left to the interior ministry or the state's civilian security and intelligence agencies[11]. The basic idea is that defence ministries provide defence against other states and the threats emanating from them, such as by intelligence gathering, while interior ministries or civilian intelligence and security agencies deal with the issue of terrorism as part of protecting public safety and fighting crime. Nonetheless, an umbrella organisation for information sharing, coordinating and de-conflicting activities would still likely be needed.

While the primary target of counterintelligence is not terrorism (and vice versa, the primary counterterrorism target is not a foreign intelligence service), their activities do sometimes overlap and the information collected can be of interest to agencies engaged in either role. As time-urgent information is needed more in counterterrorism, many countries have created 'counterterrorism centres' where information can be stored and accessed by different agencies (Riedel, 2016). For more comprehensive information exchange, de-confliction and coordination of various national security-related issues and activities, the creation of 'fusion centres' or 'information and coordination bodies' is also likely to be effective (Britovšek & Čretnik, 2016).

An important issue is the balance between the 'law enforcement model' and 'intelligence model', namely between intelligence and police powers. Here countries' strategies vary, with some trying to expand the 'intelligence model' and others trying to expand the 'law enforcement model'. But issues arise mainly from gathering intelligence and transforming it into evidence that can then be used in courts and the criminal justice system. One solution may be to combine intelligence and police powers within a single organisation. The need to merge the role of intelligence and law enforcement seems more apparent in counterterrorism than counterintelligence, where it has spurred the evolution of policing concepts and practices, such as into intelligence-led policing (Ratcliffe, 2016) or anticipative criminal investigations (Hirsch Ballin, 2012).

Although the Parliamentary Assembly of the Council of Europe (1999) recommended separating security intelligence tasks from those assigned to the police, a considerable number of liberal democracies still do not make this distinction (European Union Agency for Fundamental Rights, 2015; Vitkauskas 1999). Of course, the more power these agencies have, the more oversight, control and safety features the system must also incorporate. One such feature is different legislation covering constraints on surveillance versus criminal investigation. The oversight would need to be focused on the point where an intelligence-gathering activity transforms into a criminal investigation, so as to separate information

11 *Although civilian security-intelligence agencies are often subordinated to the ministries of interior, there are instances where they are subordinated directly to the prime minister.*

derived from intelligence gathering versus from criminal investigations. The other solution, especially in the counterterrorism context, is a security service focused on gathering intelligence but with close cooperation with a special police unit responsible for sting operations, arrests and criminal investigation of suspects.

5 CONCLUSION

To sum up, counterintelligence and counterterrorism are both important parts of national security and, while they seem very similar at first glance, they do differ from each other in certain significant respects. They both lie on a spectrum between the 'law enforcement model' and the 'intelligence model', depending on the cultural, institutional and legal structures of a state, and depending on the environment and states' perception of threats. They can overlap in certain circumstances. In the context of the 'intelligence model', they both utilise surveillance and intelligence analysis, although in the 'law enforcement model', in the case of criminal investigations, threats are considered as criminal acts and information must be presented as evidence in courts. Another overlap exists when foreign states are involved in terrorism, or when non-state terrorist groups are involved in intelligence gathering.

Both counterintelligence and counterterrorism can be divided into defensive and proactive roles. The defensive role focuses on protecting sensitive information in the case of counterintelligence, and vulnerable targets in the case of counterterrorism. Measures can overlap but they more often differ due to the risks that arise from failure in each respective activity.

The focus on different threats also means dealing with different risks in the case of failure. The imminent risk in counterintelligence is the loss of information, while the imminent risk in counterterrorism is the loss of life. Other differences arise from these differences, such as the urgency of action, or time considerations. In the case of counterintelligence, time can be an ally, while in counterterrorism time is the enemy, meaning counterintelligence can take a longer time, study an opponent and enhance security measures, while counterterrorism must act swiftly in order to save lives.

This is where the principles of the 'need to know' (which is essential in counterintelligence) and the 'need to share' information (which is essential in counterterrorism) collide. The tension between these principles causes frictions and inefficiency when states' counterintelligence and counterterrorism are organised within the same institution. Dealing with foreign states is not the same as dealing with non-state groups or individuals, especially when the main aim of the latter is to cause as much physical harm as possible.

We therefore derived four principles that should be considered when implementing counterintelligence and counterterrorism in the states' national security systems: (1) the 'intelligence model' is needed for identifying threats and assessing risks; (2) the 'law enforcement model' is needed to lawfully disrupt and prosecute suspects; (3) the 'need to share' principle is essential in counterterrorism, while the 'need to know' principle is vital for counterintelligence; and (4) time is critical for counterterrorism, but less important in counterintelligence.

The main idea of these principles is to separate counterintelligence and counterterrorism at the state level. The first solution is to leave counterintelligence as part of the traditional intelligence and security services while establishing a new organisation to work exclusively on counterterrorism. The other solution and perhaps a more practical proposal, especially for smaller states, is for the defence ministry or its intelligence and security apparatus to take over the role and responsibilities of counterintelligence, while the interior ministry or civilian security service takes over the role and responsibilities of counterterrorism. Due to the hybridisation of threats and their frequent overlaps, coordination and information sharing among different services would remain vital. A coordinating umbrella body or 'fusion centre' would likely be needed to fulfil these tasks effectively.

To conclude, the most important aspect of developing and implementing the solutions presented in this paper is understanding the threats and organisational issues related to them. The need to share information, the urgency of action and the risks of failure differ between counterintelligence and counterterrorism and, while both activities have an important role to play in the overall national security system, their varying functions and characteristics must be recognised to create and develop an organisational and legal environment in which these roles can be fulfilled effectively and appropriately.

REFERENCES

Adams, N., Nordhaus, T., & Shellenberger, M. (2011). *Counterterrorism since 9/11: Evaluating the efficacy of controversial tactics*. Oakland: The Breakthrough Institute. Retrieved from https://thebreakthrough.org/images/pdfs/CCT_Report_revised-3-31-11a.pdf

Azani, E. (2013). The hybrid terrorist organization: Hezbollah as a case study. *Studies in Conflict & Terrorism, 36*(1), 899–916.

Bauer, A. (September 13, 2016). *Who is the enemy? Terrorism as an unidentified fighting object.* International Institute for Counter-Terrorism. Retrieved from https://www.ict.org.il/Article/1774/who-is-the-enemy-terrorism-as-an-unidentified-fighting-object#gsc.tab=0

Berkowitz, B. (February 2, 2003). The big difference between intelligence and evidence. *The Washington Post*. Retrieved from https://www.washingtonpost.com/archive/opinions/2003/02/02/the-big-difference-between-intelligence-and-evidence/b589df3b-b735-4c40-8177-b5358331a690/?utm_term=.cef76f231090

Best, A. R. (2011). *Intelligence information: Need-to-know vs. need-to-share*. Washington: U.S. Congressional Research Service. Retrieved from https://fas.org/sgp/crs/intel/R41848.pdf

Bigo, D., Carrera, S., Hernanz, N., & Scherrer, A. (2015). *National security and secret evidence in legislation and before the courts: Exploring the challenges* (CEPS Liberty and Security in Europe Papers, no. 78). Brussels: Centre for European Policy Studies. Retrieved from https://www.ceps.eu/system/files/No%2078%20National%20Security%20and%20Secret%20Evidence.pdf

Britovšek, J. (2017). *Zasebna obveščevalna dejavnost v Republiki Sloveniji – teoretični, pravni in praktični vidiki* [Private intelligence in the Republic of Slovenia – a theoretical, legal and practical perspectives] (Doctoral dissertation). Ljubljana: Fakulteta za varnostne vede.

Britovšek, J., & Čretnik, A. (2016). Obveščevalno-varnostni sistem Republike Slovenije: Reorganizacija in sistemske rešitve [Intelligence and security system of the Republic of Slovenia: Reorganisation and systemic solutions]. *Varstvoslovje, 18*(3), 325–348.

Britovšek, J., Sotlar, A., & Tičar, B. (2017). Private intelligence in the Republic of Slovenia: Theoretical, legal, and practical aspects. S*ecurity Journal, 31*(2), 410–427.

Crelinsten, R. (2014). Perspectives on counterterrorism: From stovepipes to a comprehensive approach. *Perspectives on Terrorism 8*(1), 1–14

Duvenage, P. C., & Von Solms, S. H. (2015). Cyber counterintelligence: Back to the future. *Journal of Information Warfare, 13*(4), 42–56.

Eijkman, Q., & van Ginkel, B. (2011). Compatible or incompatible: Intelligence and human rights in terrorist trials. *Amsterdam Law Review, 3*(4), 3–16.

European Union Agency for Fundamental Rights. (2015). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU*. Luxembourg: Publications Office of the European Union.

Fakhoury, A. (2017). Persona Non Grata: The obligation of diplomats to respect the laws and regulations of the hosting state. *Journal of Law, Policy and Globalization, 57*. Retrieved from http://www.iiste.org/Journals/index.php/JLPG/article/viewFile/35178/36182

Gleghorn, E. T. (2003). *Exposing the seams: The impetus for reforming U.S. counterintelligence* (Master's thesis). Monterey: Naval Postgraduate School.

Goitein, E., & Shapiro, M. D. (2011). *Reducing overclassification through accountability*. New York: Brennan Center for Justice. Retrieved from http://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf

Harber, R. J. (2009). Unconventional spies: The counterintelligence threat from non-state actors. *International Journal of Intelligence and CounterIntelligence, 22*(2), 221–236.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.

Hirsch Ballin, F. H. M. (2012). *Anticipative criminal investigation: Theory and counterterrorism practice in the Netherlands and the United States*. The Hague: T.M.C. Asser Press.

Hoffman, B. (2006). *Inside terrorism* (2nd ed.). New York: Columbia University Press.

Hulnick, S. A. (1997). Intelligence and law enforcement: The 'Spies Are Not Cops' problem. *International Journal of Intelligence and Counterintelligence, 10*(3), 269–286.

Liulevicius, G. V. (2011). *Espionage and covert operations: A global history*. Chantilly: The Teaching Company.

Lockwood, N. (December 23, 2011). How the Soviet Union transformed terrorism. *The Atlantic*. Retrieved from https://www.theatlantic.com/international/archive/2011/12/how-the-soviet-union-transformed-terrorism/250433/

Lubin, A. (January 9, 2017). A new era of mass surveillance is emerging across Europe. *Just Security.* Retrieved from https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/

Lutwak, N. E. (December 17, 2015). Italy has lessons to teach in counterterrorism. *Nikkei Asian Review*. Retrieved from https://asia.nikkei.com/Politics/Edward-N.-Luttwak-Italy-has-lessons-to-teach-in-counterterrorism

Marone, F. (March 13, 2017). *The use of deportation in counter-terrorism: Insights from the Italian case.* The Hague: The International Centre for Counter-Terrorism. Retrieved from https://icct.nl/publication/the-use-of-deportation-in-counter-terrorism-insights-from-the-italian-case/

McGowan, L. (2014). Right-wing violence in Germany: Assessing the objectives, personalities and terror trail of the national socialist underground and the state's response to it. *German Politics, 23*(3), 196–212.

Miller, H. B. (2011). Commentary, The death of secrecy: Need to know . . . with whom to share. *Studies in Intelligence, 55*(3). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-3/the-death-of-secrecy-need-to-know...with-whom-to-share.html

Mobley, W. B. (2012). *Terrorism and counterintelligence: How terrorist groups elude detection*. New York: Columbia University Press.

Parliamentary Assembly of the Council of Europe. (1999). *Control of internal security services in council of Europe member states*. Strasbourg: Council of Europe. Retrieved from http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en

Pedahzur, A. (2009). *The Israeli Secret Services and the struggle against terrorism*. New York: Columbia University Press.

Peter, L. (July 26, 2016). How France is wrestling with jihadist terror. *The BBC*. Retrieved from http://www.bbc.co.uk/news/world-europe-36902332

Podbregar, I., & Ivanuša, T. (Eds.). (2016). *The anatomy of counterintelligence: European perspective.* Sharjah: Bentham Science.

Priest, D. (November 13, 2017). Russia's election meddling is another American intelligence failure. *The New Yorker*. Retrieved from https://www.newyorker.com/news/news-desk/russias-election-meddling-is-another-american-intelligence-failure

Prunckun, H. (2012). *Counterintelligence theory and practice*. Lanham: Rowman and Littlefield.

Prunckun, H. (2014). Extending the theoretical structure of intelligence to counterintelligence. *Salus Journal, 2*(2), 31–49.

Ramsay, G. (2015). Why terrorism can, but should not be defined. *Critical Studies on Terrorism, 8*(2), 211–228.

Ratcliffe, H. R. (2016). *Intelligence-led policing* (2nd ed.). London; New York: Routledge.

Richards, A. (2014). Conceptualizing terrorism. *Studies in Conflict and Terrorism, 37*(3), 213–236.

Riedel, B. (July 18, 2016). France needs its own National Counterterrorism Center. *Brookings*. Retrieved from https://www.brookings.edu/blog/order-from-chaos/2016/07/18/france-needs-its-own-national-counterterrorism-center/

Roach, K. (2015). Introduction: Comparative counter-terrorism law comes of age. In K. Roach (Ed.), *Comparative counter-terrorism law* (pp. 1–45). Cambridge: Cambridge University.

Schmid, A. (2004). Terrorism: The definitional problem. *Case Western Journal of International Law, 36*(2), 375–419.

Treverton, F. G. (2009). *Intelligence for an age of terror*. Cambridge; New York: University Press.

Van Cleave, K. M., (2013). What is counterintelligence? A guide to thinking and teaching about CI. *The Intelligencer, 20*(2), 57–65.

Vandepeer, C. (2011). *Intelligence analysis and threat assessment: Towards a more comprehensive model of threat*. Perth: Edith Cowan University. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1020&context=asi

Vitkauskas, D. (1999). *The role of a security intelligence service in a democracy*. North Atlantic Treaty Organisation. Retrieved from https://www.nato.int/acad/fellow/97-99/vitkauskas.pdf

Warner, M. (2002). Wanted: A definition of 'intelligence'. Understanding our craft. *Studies in Intelligence, 46*(3). Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-46no3/article02.html

Warner, M. (2014). *The rise and fall of intelligence: A international security history*. Washington: Georgetown University Press.

Weinberg, L., Pedahzur, A., & Hirsch-Hoefler, S. (2004). The challenges of conceptualizing terrorism. *Terrorism and Political Violence, 16*(4), 777–794.

About the Author:

Jaroš Britovšek, PhD, is employed by the Ministry of Defence of the Republic of Slovenia. E-mail: jaros.britovsek@mors.si