

Journal of Contemporary European Research

Volume 9, Issue 1 (2013)

Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?

Aleš Završnik *Institute of Criminology, Ljubljana*

Citation

Završnik, A. (2013). 'Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?', *Journal of Contemporary European Research*. 9 (1), pp. 181-202.

First published at: www.jcer.net

Abstract

To an ever-increasing extent, law enforcement agencies work with and rely on information obtained and passed to them by intelligence services. However, in comparison to the police, intelligence services face much less regulation or supervision. Contrasting levels of regulation and supervision pose a problem where the institutional and functional borders between intelligence and police agencies are increasingly blurred. For example: new 'hybrid' police-intelligence institutions have sprung up; information is freely exchanged between police and intelligence organisations; and information gathered by intelligence agencies is used in criminal proceedings. But an impulsive blurring of organisational boundaries is not a solution to growing fears of terrorism and serious cross-border crime. Secret or sensitive information should be used in a way that balances the need for intelligence gathering with the right of the defence to examine incriminating evidence.

Keywords

Law enforcement; intelligence; boundaries; criminal procedure; European Court of Human Rights; surveillance; Central and Eastern Europe; Slovenia

The boundaries between different agencies in the control and security domain – organisations such as the administrative authorities, special inspection services, municipalities, the police, intelligence services, the army, private security services and non-governmental organisations – are becoming increasingly indistinct (Bigo 2005; Loader 2002; Bayley & Shearing 2001). This blurring has produced what some describe as a state of 'security androgyny' (Easton et al. 2010) where the military adopts a more constabulary role (Easton et al. 2010), the police adopts a paramilitary role and shifts towards an intelligence-type of *modus operandi*, while intelligence work becomes ever more engrained in everyday law enforcement, of which internal security challenges take up a growing share (Lutterbeck 2005).

The merging or overlapping of powers between law enforcement and intelligence agencies raises deep concerns about contemporary public policy and civil liberties. Together with other shifts in the field of security (e.g. privatisation) the blurring may well lead to a state of arbitrary 'feudal security' (cf. Wakefield 2005). The issue addressed here is thus whether the erosion of boundaries between police and intelligence agencies can undermine the rule of law and infringe disproportionately and unnecessarily upon civil liberties. More specifically, the present article will address the question of whether and how the police can bend the rules of criminal procedure by making intelligence information available for use in court. From the perspective of intelligence agencies, this means considering their new role in domestic security, their relationship to the police and their freedom from the mechanisms which regulate police operations.

The institutional separation of law enforcement and internal security from (foreign) intelligence gathering in most cases predates the Second World War (Sweet 2010). The line was drawn firmly by most countries after the Second World War. Subsequently, the Cold War had enormous impact on the way security institutions themselves and the boundaries between them developed (cf. Janssens 2010; Broesder et al. 2010; De Weger 2010; Lutterbeck 2005; Bigo 2000; Kraska 1996). When the USA, for instance, established the Central Intelligence Agency (CIA) within the National Security Act of 1947, the act required that the CIA have no police, subpoena, or law enforcement powers or internal security functions. Meanwhile Central and Eastern European (CEE) countries on the other side of the Iron Curtain separated their security actors with a similar dividing line. Police agencies were to be concerned with internal security, while secret intelligence services occupied themselves with threats to national security from

'the enemy outside'. The question of the proximity of these two fields resurfaced in the CCE region after the collapse of the centralised authoritarian regimes in the 1990s, as new democracies attempted building political systems based on the rule of law and respect for fundamental human rights and liberties.

Almost everywhere one looks on either side of the Iron Curtain, in the USA from the 1970s and in CEE countries from the 1990s, liberal democracies tended to construct a strong 'information wall' between intelligence and law enforcement. Moreover, law enforcement was conceived as being a mainly reactive activity, and foreign intelligence as a proactive one. But later, at the beginning of the twenty first century and most notably after the terrorist attacks in New York, Madrid and London, the boundaries started to shift again and the separation between security actors became blurred.

Seen from a longer historical perspective, the current relaxation of borders in the control and security domain is not at all new. The influence of different agencies has varied over time and so has the kind of work they carry out. A full account of these evolutions is obviously beyond the scope of the present discussion. The focus here will thus be on how law enforcement and foreign intelligence work has overlapped, in institutional, functional, operative, technological and spatial terms, over the last two decades. We may summarise the resulting blur as follows: institutionally, new hybrid agencies and organs have been formed to facilitate cooperation and information exchange. In spatial terms, law enforcement agencies have started focusing on external threats in 'peacekeeping and stabilisation operations' (cf. Last 2010) while intelligence agencies began turning to domestic threats. In functional and operative terms 'intelligence-led policing' is increasingly the prototype of all police work (cf. Lemieux 2008) and police forces have been permitted to employ more invasive secret service-type powers (examples would include digital searches with on-line 'Trojan horses' that fall outside the scope of judicial overview¹ and video surveillance enhanced with face-recognition or registration plate-recognition systems).²

The blurring of these boundaries cannot be assessed simply as a positive or negative development. It can be interpreted in several contradictory ways: as complementary or competitive; as a trend providing a security net; or one demolishing the safety net of human rights. Hermetically sealed dividing lines between police and intelligence lead to unjustifiable inefficacy and inefficiency on both sides, and agencies should obviously be allowed to exchange relevant information. But the examples to be outlined in this paper will show that impulsively blurring the boundaries between these fields is not a solution to growing fears of terrorism, cross-border crime and irregular migration. Walls torn-down raise the level of 'emergency criminal law' (Vervaele 2005) and lead us towards a 'pre-crime society' (Zedner 2007).

This paper does not consider the numerous other ways in which the boundaries between security actors are growing more indistinct, notably with the growing involvement of military forces in domestic security operations (the 'constabularisation' of the military). This is seen when armed-forces personnel undertake work developed in and for peacetime situations, such as supporting civilian crisis management activities, enabling the return of refugees, supporting elections, developing and maintaining infrastructure and even escorting children on field trips or to schools (den Boer et al. 2010: 224). The article also does not cover the increasingly important issues of intelligence obtained from private parties and the privatisation of the intelligence network itself.

Instead, the article will begin by reviewing the state of existing research in the fields of International Relations and Public Policy about security actors and changes they face in contemporary liberal democracies. A more descriptive approach at the beginning of the discussion will then seek to paint a 'bigger picture' of the institutional changes seen in the control and security domain. The pages below then continue with a brief historical overview of how the boundaries between two selected security actors have developed. In order to avoid a more general discussion about overall trends in western liberal

democracies, the article offers two country-specific case studies. The first deals with the case of boundaries fading between two security actors in the USA, which contains the largest network of intelligence services in the western world and has served as a model for many of the world's 'emerging democracies' and 'transitional' countries. Additionally, as a protagonist in the Cold War the USA had paramount influence in the development of (foreign) intelligence around the globe. The second case study presents the blurring of police and secret service activity from the CEE region, specifically the former Yugoslavia and one of its successor-states, the Republic of Slovenia. A pragmatic reason for the selection is that the shifts being analysed here have been extremely understudied in the CEE region (except with regard to the situations in the former war zones of Bosnia and Herzegovina and Kosovo). A more substantive reason is that these countries have only recently set in place new institutional arrangements for their central security actors (the police, military, intelligence and private security industry). In the 1990s and 2000s CEE countries underwent profound political, legal, economic and social changes, and, in the case of the former Yugoslavia, even warfare. After the collapse of centralised political regimes, which depending on the country and the period were mostly authoritarian, these countries were expected to copy the institutional arrangements of the countries standing on the 'free' side of the Iron Curtain. But the provision of these 'good examples' in the West then began spurring significant social, economic and technological changes of their own. The 'Western' prototypes for 'Eastern' application were themselves being profoundly revised in the face of new types of 'asymmetrical' security threats – threats posed by non-state actors, terrorism, globalised organised crime, aided in part by a revolution in information technology which brought means of surveillance beyond the dreams of the Stasi or UDBA.

Moving on from these case studies, the article then turns to the means being used to create and exploit the overlap of police and intelligence. It shows how institutional blurring is occurring in the form of new hybrid police-intelligence institutions, through enhanced cooperation and intensified information sharing and exchange between law enforcement and intelligence agencies. It also traces the way intelligence agencies have begun addressing internal security at the same time as new intelligence-style modus operandi have been adopted by the police. In attempting to answer the question posed in its title, the article then moves on to focus in more detail on the use of information gathered by intelligence agencies in criminal proceedings. From there it tackles the changes the two selected security actors face from a legal perspective, or more precisely, from a criminal law perspective. It considers overview mechanisms in cases where intelligence services provided crucial information to law enforcement agencies. The 'information laundering' (Vervaele 2005) which results from this state of affairs is presented as an outcome of the information wall between police and intelligence being demolished; and as such the reason why the overlapping of police and intelligence activity must be seen as a harmful policy so far as civil liberties are concerned.

EXISTING RESEARCH ON DISAPPEARING BOUNDARIES BETWEEN SECURITY ACTORS

It has been noted frequently in recent years how the security landscape is 'changing profoundly' (e.g. Easton et al. 2010) and how the boundaries between actors within the control and security domain are blurring, overlapping or disappearing altogether. Attention has been drawn to the important questions such trends raise with regard to legal safeguards and respect for human rights (Easton et al. 2010; Andreas and Price 2001). Several of the essays collected in Easton et al. (2010) examine aspects of the blurring boundaries, but focus particularly on how the military is undergoing a process of constabularisation at the same time that the police are experiencing one of militarisation. The focus of several parts of the book is on how the roles of the two have evolved in peacekeeping and stabilisation operations (e.g. Janssens 2010, Last 2010).

The book also tackles the various types of constabulary force employed as 'bridging actors' between the police and military (Neuteboom 2010).

Others (O'Neill, Léonard and Kaunert 2011) point out how security policy developments in Europe have been breath-taking both in speed and scale, and how institutional rearrangements in the EU have gone hand-in-hand with theoretical developments in Security Studies. The definition of security as referring to the security of the state, as threatened by the military power of other states and defended by the military power of the state in question (Mutimer cited in O'Neill et al. 2011), is now widely viewed as being inadequate to cover the changing international environment that developed after the Cold War. Since then Security Studies has been dominated by the so-called widening-deepening debate, in which the widening dimension has focused on the extension of security to other issues or sectors beyond traditional military concerns, while the deepening dimension has questioned whether entities other than the state – such as the EU, for example – should be able to claim they suffer security threats (Krause and Williams cited in O'Neill et al. 2011). These authors raise an important question for future research: why is it that some issues come to be socially defined as matters of security while others escape securitisation?

The traditional institutional divides began changing as longstanding notions of internal (domestic) and external (international) threats became obsolete. As noted by Bigo (2005, 2000), today we are witnessing a transnationalisation of security and this in turn has had far-reaching consequences for the rearrangement of the respective roles of internal and external security agencies. But as Lutterbeck (2005: 232) also critically observed, this had a profound effect on all security actors, although the research literature to date has only been able to tackle in-depth the shifts affecting policing and the domestication (also policisation or constabularisation) of the military. This gap is therefore one the present article begins to fill.

Notwithstanding the lack of detailed study, a few scholars have considered the blurring of law enforcement and intelligence agencies at a more or less introductory level. Focusing exclusively on intelligence activities and agencies in Europe, Svendsen (2011) observes that in the early twenty first century we witnessed greater levels of intelligence co-operation than seen previously. He highlights 'a plethora of overlapping international intelligence liaison arrangements' (Svendsen 2011: 537) that he groups in three broad categories: bilateral relationships, multilateral Europe-centred arrangements for national intelligence services (e.g. Club de Berne, the Counter Terrorist Group formed after 9/11, the Middle European Conference, the plethora of NATO's overlapping intelligence-associated arrangements, Open source intelligence (OSINT) partnerships) and a category encapsulating the European Union's intelligence arrangements, which allow for pockets of specialist intelligence liaison within the EU framework as part of the EU's Common Foreign and Security Policy and, as of 2010, the Common Security and Defence Policy (e.g. the EU Satellite Centre (SatCen), the Joint Situation Centre (SitCen), the EU Terrorism Working Group, MONEYVAL).

The increasing proximity of law enforcement and foreign intelligence activities has received some attention in analysis of the post-Cold-War United States. For instance, Andreas and Price (2001) claim that the American 'national security state' has increasingly been transformed from a 'war-fighting' state into one focused on 'crime-fighting' and that this shifting security agenda has led to the growing convergence of law enforcement and foreign intelligence. Lutterbeck (2005), on the other hand, analysed internal and external security in Europe and distinguished three shifts toppling the wall between the two security actors: a shift in the focus of foreign intelligence agencies towards internal (or transnational) security challenges, enhanced cooperation between intelligence services and law enforcement bodies, and a shift towards intelligence-style modus operandi by police agencies (Lutterbeck 2005: 238–241).

Others have tackled the leaky boundaries between police and intelligence from the perspective of a pluralisation of policing (Loader, 2000) or 'plural policing' (Crawford et al. 2005). In discussing the 'enhanced policing capacity in Europe', Loader (2002: 133) observes that the 'core business' of the supranational institutions, such as the European Police Office (Europol) or the European Public-Prosecutors' Office (Eurojust), lies precisely in the 'exchange of information and intelligence'. Similarly, the enhanced policing capacity seen across Europe in the wake of intergovernmental co-operation is attributed to policing efforts being centralised and co-ordinated. For example, intelligence on criminal activities has become shared more efficiently than before, and there has been the creation of a transnational police elite orientated to 'forging common 'solutions' to common 'security' problems' (Loader 2002: 133).

To sum up, the existing literature has tackled the following changing roles between security actors with respect to: (1) a constabularisation or policisation of the military (Broesder et al. 2010; Easton et al. 2010); (2) a militarisation of policing (Last 2010; Kraska 2007; Lemieux and Dupont 2005); (3) an increasing role played by the intermediary actors filling the 'security gap' between military and police, such as gendarmerie forces (see Neuteboom 2010); (4) an increasing role taken on by private security companies in peace-keeping operations and increasingly in domestic settings (Završnik 2012); (5) a policisation of foreign intelligence work (Lutterbeck 2005); and, (6) an 'intelligence-isation' of policing (e.g. Lemieux 2008).

The disappearing boundaries between security actors should be distinguished from the boundaries between security areas (border control, police, defence, intelligence, prison and justice reform etc.). For analytical purposes, it is important to note that the former is an organisational divide, while the latter addresses functions that actors execute. The convergence can thus be observed at different levels, such as at a functional level (e.g. the growing involvement of intelligence services in domestic security missions), an operative level (the police becoming more proactive) and a technological level (with the police increasingly using surveillance technologies).

The present article contributes to existing scholarly work by providing additional case studies to illustrate the disappearing boundaries between law enforcement and intelligence agencies from CEE countries. By comparing the institutional arrangements of the selected security actors from behind and in front of the Iron Curtain, the article will highlight some trans-national features of the two institutions that transcend the national specifics I shall turn to in the following sections. By comparing two examples from both sides of the Cold War divide, it will become clear that the fundamental issue in such institutional reconstruction work is how two legitimate interests can be balanced: namely the state's interest in providing security on the one hand and the individual's right to due process of law on the other. The proximity between law enforcement and intelligence agencies is a matter of degree and dependent on many political, economic, even emotional (fear of crime) and other contingent factors. These factors can be shown only by looking in detail at the relevant features of a chosen state, its formation in *statu nascendi* and its international security situation. It is historical analysis of this kind that is taken up in the following section.

HISTORICAL OVERVIEW OF THE OSCILLATING BOUNDARIES BETWEEN LAW ENFORCEMENT AND INTELLIGENCE AGENCIES

A distinct concept of the police force emerged in the nineteenth century as countries sought the best means of keeping 'streets safe' that would simultaneously resemble and yet be distinct from the military and operate as a kind of 'civilised security' (Jauregui 2010). Countries separated forces providing internal security from those providing external security and some countries also formed a bridging actor in the form of a paramilitary force or gendarmerie. Generally, the police focused on internal safety and

became regulated by a legal regime of criminal procedure, while intelligence operations, such as intercepting hostile foreign communications, fell under the remit of intelligence services geared to monitor threats to national security from other states. Consequently, intelligence agencies operated only under (political) parliamentary control or very limited judicial control executed by the highest court in the jurisdiction. They have been allowed to operate under much higher degrees of secrecy in order to protect their sources. One immediate result of the lassitude with which their work was supervised was that while information gathered by the police was admitted in court as evidence, that gathered by intelligence agencies was not and could only serve as circumstantial evidence or a prompt for further criminal investigation; which would then be conducted by the police as criminal procedure dictated.

The boundaries between law enforcement and (foreign) intelligence that I claim are overlapping should thus in fact be regarded as artificial from the beginning. In other words, the law enforcement and intelligence communities have always exchanged information, although the formalisation of the exchange and legal power of the information being passed back and forth naturally varied with given periods and countries. The boundaries are, as den Boer et al. put it (2010: 226), 'a human construct that serves specific purposes, including political, and depends on the time and place in which they are active'.

The history of intelligence and law enforcement agencies described above is thus painted with a very broad brush. More detail can be offered by taking into account the specific purposes emerging at a particular a time and place. The discussion here will thus continue by presenting two examples, those of the USA and Slovenia, the world's largest and most powerful democracy and a newly established sovereign state in the north of the former Yugoslavia, which became independent in 1991. These countries are different, if not antipodal, in several aspects. They differ not only in terms of their size and age, but also their legal traditions (Anglo-Saxon v. Continental) and the sides they took in the bi-polar division of the world during the Cold War. Although technically non-aligned, Yugoslavia belonged in broader terms to what was viewed as the Communist bloc. The last factor is crucial for two reasons. Firstly, the bi-polar division of the world was sustained because countries in both blocs (together with the non-aligned group) developed very similar security institutions (and, of course, engaged in very similar activities) and secondly, the end of the Cold War was, amongst other things, a significant cause behind the disappearance of boundaries taking place today in the security domain.

Although the mainstream literature on the folding and breaking of these boundaries repeatedly documents the highly problematic domestic surveillance activities of intelligence agencies in the Eastern bloc, one should recall the intensity with which secret services in the West also kept their own populations under observation. For instance, the notorious Watergate affair disclosed the US government's involvement in domestic surveillance. Other leaks in the 1970s brought to public attention how the American surveillance community was increasingly involved in counterterrorism, counter-narcotics, and other non-proliferation activities carried out by law enforcement agencies (Manget 2007). Similar events occurred during the Cold War in Western Europe, where a secret NATO organisation called 'Gladio' was used to manipulate the political climate in many European countries, (e.g. France, Belgium, Switzerland, Italy) and to resist a Soviet invasion (Ganser 2005).

Given the extent to which intelligence agencies are involved in protecting the security of the state, as the examples of the USA and Slovenia will show, they form an inherent part of a sovereign state's authority and are never subjected to normal judicial review. What changed with the end of the Cold War was that intelligence operatives in both the Western and Eastern blocs became deprived of their main targets. This sparked a frantic search by these agencies for new fields of activity (Klerks 1993) and led to the walls between the pastures of law enforcement and intelligence being undermined and

knocked down, allowing bulls to charge freely and perhaps the occasional wolf to enter the fold. The historical background of the two countries reveals how, despite the manifold differences between them, the need for firm separation between the agencies in question was at first recognised in both blocs for very similar reasons. But let us first turn to the early United States.

Nathan Hale is usually considered the first American spy and was hung by the British during the Revolutionary War (Sweet 2010). At the time there were no laws regulating the intelligence community as a whole in America, but intelligence functions clearly existed from the time before American independence. According to Sweet (2010), intelligence in the USA has its earliest roots in the American Revolution and Benjamin Franklin could be considered the first intelligence officer operating on behalf of the United States. '[In Paris] he had a twofold mission: to get military and economic assistance from France, and to establish and run a network of agents in London following developments in the British government' (Holt in Sweet 2010: 340). This early period of unregulated intelligence in the USA is very similar to the situation in the former Yugoslavia after the Second World War and its northern successor, Slovenia, in the early nineties, as discussed next.

The organisation of intelligence in the former Yugoslavia followed the Soviet Union model, separating the regular police (Milicija) and secret police (early name OZNA, renamed UDBA in 1946 and later SDV in 1967). UDBA was an agent of communist ideology established in each of the six republics that together constituted the federal state. It was established in 1946 and abolished as SDV in 1990. During this period it underwent substantial reforms, most notably in 1952 when it ceased to be a part of the military and after abuses that surfaced in the 1960s. In 1966, the supreme political body of the federal state (Centralni Komite Zveze Komunistov Jugoslavije) claimed that the intelligence service should be strictly bound by the law (i.e. by the principle of legality) and operating within the public's oversight (Pusić 1985: 54). For an understanding of its early role, it is crucial to contextualise its position in the wider international transformations after World War II. The new Yugoslavia (SFRY) was then under enormous pressure from both the Soviet bloc and the Western countries. It was not yet a firm and cohesive entity either internally or externally. In the first 15 years after the war, UDBA's primary tasks related to domestic security, such as to discover and suppress the activities of former German collaborators, pro-monarchy forces from abroad and special agent groups that were trying to displace the governing elite and induce a coup d'état (Pirjevec 2011). After the 1948 dispute of Yugoslavia with Cominform (Communist Information Bureau – the international communist movement), i.e. between Stalin and Tito, Yugoslavia leaned to the West, but remained relatively independent of both of the blocs. It started to shape the so called 'third way' in the form of the non-aligned movement that embraced three quarters of the world population soon after its inception.

On the other hand, the Yugoslav army was another strong political actor, a state within a state which never submitted to political or any other form of review with its own intelligence service. Its engagement in political life surfaced only occasionally into public view, especially in the 1980s with the rise of critical movements in the northern Yugoslav republics of Slovenia and Croatia. The army then claimed that appeals to convert the country to a democratic political model and submit it to the checks of a civil society were threats to constitutional order and the sovereignty of the federal state, i.e. a prime intelligence domain. But the noteworthy particular in this conflict, especially with regard to the Balkan War that resulted in the 1990s, is that the Yugoslav military system consisted not only of the centralised Yugoslav People's Army (Jugoslovska ljudska armada; JLA), but included also special complementary armed divisions called the Territorial Defence Forces (Teritorialna obramba; TO) (Bolfek 2010).

The trigger for the development of the TO occurred in 1968 when the seizure of Czechoslovakia by Warsaw Pact troops gave a ferocious warning to Yugoslavia that its

military and political position was precarious in the extreme (Bolfek 2010). Having realised that Yugoslavia would not be able to defend itself from an eastern attack, the military and political establishment decided to use the fruits of experience from Partisan guerrilla warfare during World War Two. A new military protocol, 'The Doctrine of Total People's Defence' was drawn up, and the high command of the TO was established in 1968. A new system of Territorial Defence Forces was formed within republics, municipalities, local communities, and even labour organisations. The TO was different from a typical military organisation. It remained subordinate to the JLA, but the command language was local (i.e. Slovene in Slovenia and not the official Serbo-Croatian language) and the public accepted its members as soldiers of the individual republics rather than the Yugoslav federation. With the decentralisation of the federal state of Yugoslavia in 1974, the TO was further transformed to constitute the armed forces of particular Yugoslav republics, setting the conditions for the new separate republican armies which became so active in the 1990s (Bolfek 2010).

These two armies and their parallel intelligence agencies significantly marked the dissolution of the federal Yugoslavia in the 1990s. When the federal authorities issued an order commanding TO units to surrender their arms to the JLA (issued on 15 May 1990), some TO units did hand over their weapons, but many of those established within municipalities and local communities refused to comply. In response to the order to disarm, a group in Slovenia called the 'Network for the Deployment of National Protection Forces' (Manevrska struktura narodne zaščite; MSNZ) was formed from a group of police officers (Milicija) and TO members who came under the command of the Republican Secretariat of Defence and Republican Secretariat of the Internal Affairs. This armed formation secured the country three months later by repelling an attack from the JLA, thereby safeguarding the independence of Slovenia. The activities labelled as crimes against the constitutional order were viewed *ex post facto* as heroic acts establishing a new independent state.

This brief historical overview shows how the boundaries between different actors within the control and security domain are predominantly determined by circumstances, time and place. The position a particular agency occupies in the control and security domain is always the result of how that domain has evolved in a particular country. Countries in *statu nascendi* tend to rely increasingly on intelligence activities both to provide internal stability and to secure the state's place in the international order of states. In both countries one can discern the type of 'pre-legal violence' conducted by the intelligence agencies establishing the law, as described by Walter Benjamin in his opus. Only gradually, as the crisis situation subsides, is it possible for the intelligence and police to go their separate ways (e.g. after 1952 in former Yugoslavia). When this separation does occur, in a democratic country the bulk of the intelligence community remains in some connection with the armed forces, with each branch of the military retaining its own intelligence departments and personnel.

Returning to our two examples, it should go without saying that there are innumerable differences, qualitatively and quantitatively, between the security domains of Slovenia and America. A general pattern is discernible nonetheless in a common effort to segregate the fields of law enforcement and military intelligence. However, over the past dozen years or so, that segregation has been placed under great strain in both countries (Best 2007 in Sweet 2010: 340): cross-border crime, organised crime and the sensational terrorist attacks at the beginning of the new millennium set in motion a process which has brought the separate agencies closer again. The question to be addressed in a later section is how the regulation of their work has evolved. As we shall see, the proximity of both actors led to very similar safeguards and checks being set in place in both the United States and Slovenia, and also at a European level by the European Court of Human Rights. But first let us verify the thesis that law enforcement and intelligence are indeed becoming ever more closely intermeshed: where is the linkage between the agencies most manifest?

WAYS IN WHICH THE LINES BETWEEN LAW ENFORCEMENT AND INTELLIGENCE AGENCIES ARE DISAPPEARING

Proximity through hybrid institution and omnibus legislation

It was found that security actors could be brought closer together by forming new hybrid institutions to connect them. Such institutions began to emerge extensively at the beginning of the twenty first century in the majority of European countries (Lutterbeck 2005) and the United States. The main justification for such institutional rearrangements was that they would foster information sharing and provide separate institutions with stronger and more integrated analytical expertise.

To improve cooperation between law enforcement and intelligence communities, the US Department of Justice created the Executive Office for National Security. This coordinates those activities of the Justice Department that involve national security issues, acts as a forum for developing national security policy and serves as a focal point linking the Justice Department with other agencies on matters of national security. Other new institutional mechanisms to facilitate better collaboration in the US context include the Intelligence-Law Enforcement Policy Board, co-chaired by the deputy director of the CIA and the deputy attorney general, the joint Intelligence-Law Enforcement Working Group, and the Special Task Force on Law Enforcement/Intelligence Overseas (Andreas and Price 2001).

The post-socialist process of economic, political and social transition which Slovenia underwent put the smaller country in a different position. Marked by ruthless privatisation and the denationalisation of once public property, with relatively high rates of systemic corruption, the newly established state lacked the resources and political determination to transform completely the institutional arrangement of its security actors that had existed at least from the 1960s onwards. It seems that the governing elite did not have an interest in establishing strong security apparatuses. UDBA was disbanded, but at the same time the newly established intelligence agency (SOVA) was left in a relatively weak position: secret documents were stolen from archives, agent networks revealed to the public etc. If other countries changed intelligence agencies into overwhelming ('dangerous') domestic security actors by deepening (e.g. with new powers in existing working areas) and widening (in the domestic domain) their powers, the newly established state has not been able to replace the old intelligence agency with a strong but democratically confined guardian of national interests. The example of the National Bureau of Investigation created in 2010 shows how even less ambitious projects to adapt law enforcement to the increasing problems of corruption, organised crime and other serious cross-border crime have been blocked.

The motive for the formation of the Bureau was to increase the efficiency, efficacy and autonomy of law enforcement in detecting and investigating serious criminal offences, for example, economic and financial crime, through a multidisciplinary approach in the form of a one-stop office with special investigation teams based at the same location. It was also conceived as a body to co-ordinate other institutions (the Tax Administration, the Customs office) on a national and international level. But despite the Bureau being merely a new criminal investigation unit of the General Police Administration, positioned within the Criminal Police Directorate, it already faces governmental criticism on account of its autonomy.³ Since the future of a criminal investigation unit within the police is itself uncertain, enhanced cooperation between the law enforcement and intelligence communities or substantial institutional rearrangements seem very distant options, a crucial aspect for the arguments advanced in this article.

The institutional arrangement of security actors should provide a proper balance between competing interests and not neglect interests, either by tearing down the institutional and functional divides between security actors and putting civil liberties at risk or, as the Slovenian example shows, by limiting the state's legitimate interest in

providing national security. The other means of increasing proximity between security actors is the use of special omnibus legislation that traverses and amends numerous regulations from a certain perspective or in pursuit of a set objective. The USA PATRIOT Act 2001,⁴ rushed through Congress in October 2001, has been understood by many as 'the most wide-ranging law passed in recent memory' (Sweet 2010: 343). The act gave the government significant new powers to conduct electronic surveillance of the internet and to foster information collection and information sharing. It granted the government wider authorities, enhanced surveillance techniques, and enabled swifter prosecutions and the imposition of severer sentences. This was achieved by amending at least 12 federal statutes, mandating dozens of new reports, and directly appropriating USD 2.6 billion (Sweet 2010).⁵

The shift of intelligence towards internal security

The policisation of foreign intelligence agencies started in the early 1990s when intelligence agencies in European countries entered various new domains previously regarded as the preserve of the police. The Slovenian Intelligence and Security Agency (SOVA) moved towards internal security challenges with amendments adopted in 2003, although these changes did not significantly alter the direction of the overall trend of undermining the power and reputation of the new agency.

But there was another unfortunate practice of the agency related to the transition period. As we shall see later, there was a secret arrangement between SOVA and the police allowing the former to monitor electronic communications that should in fact only have been available to the police. But in general, SOVA's remit was to provide intelligence relevant for safeguarding the security, political and economic interests of the state from *foreign* threats only until 2003. But the amending provisions now empower SOVA to conduct *domestic* surveillance of telecommunications, albeit under the supervision of the President of the Supreme Court of Slovenia.

The extension of the Slovenian central intelligence and security service into the domestic security domain nevertheless offers another insight into the possible consequences of relaxing or removing institutional boundaries. Intelligence services can also suffer from loss of (distinct) powers and identity. A close reading of the Slovene Intelligence and Security Agency Act (the SOVA Act hereafter) amended in 2006 indicates that SOVA's shift into the domestic realm was accompanied by an increasing 'juridicisation' of its activities. This, I suggest, not only goes hand-in-hand with the overall trend of undermining the power of the new Slovenian intelligence agency, but also shows how *any* intelligence agency can suffer from loss of distinct identity when moving into the new security domain. For instance, a request from SOVA to intercept the telecommunications of an identifiable individual must be approved by the judiciary (here the President of the Slovenian Supreme Court) and not just by the director of the agency. Furthermore, it can only be authorised by a 'written order issued for each individual case', if it is 'very likely' that the security of the state is at risk (Article 24 of the SOVA Act). The introduction of a standard of proof that the agency must meet in order to obtain this written order also pushes the intelligence agency closer to the restraints and regulations placed on law enforcement. There is no doubt that as its sphere of operation comes to encompass domestic security, the intelligence service should be subjected to increased judicial review, to the same extent as law enforcement agencies. But this can also cripple the service's surveillance powers and also open to question why a separate intelligence service should exist at all.

The shift of intelligence towards the field of internal security is similar in the USA. According to Andreas and Price (2001: 41), the government started using rhetoric explicitly in favour of changing the 'traditional' domains of intelligence employment as early as July 1995, when President Clinton ordered intelligence agencies to prioritise

such 'transnational threats' as organised crime in addition to their traditional concerns. The new CIA orientation towards domestic security is reflected in the establishment of the Director of Central Intelligence (DCI) Crime and Counter-Narcotics Center where Drug Enforcement Administration and FBI agents are assigned to work with the CIA (Andreas and Price 2001: 41).

The shift of police towards intelligence

The 'intelligence-isation' of police agencies should be read in the sense that they have been resorting to ever more sophisticated surveillance technology in recent years, and have been granted much more intrusive investigative powers in order to use it. In doing so they have brought their modus operandi closer to that of intelligence agencies (Lutterbeck 2005:240). Technologically enhanced surveillance is changing policing into an 'almost entirely informationalised activity' (Loader 2002: 142). This turn goes together with the new tendencies towards creating a 'pre-emptive' criminal justice model (Zedner 2007) or 'preventive law enforcement' (Cole and Lobel 2007) whereby criminal justice actors are orientated not only to crimes already committed, but also to detecting the perpetrators of crimes that have yet to take place. Increasingly, the police 'trawl' through databases in order to match the names they contain against a pre-determined profile. Such police searches are commonly intelligence-led – based on secret information beyond the reach of legal contestation and carried out as part of European (rather than just national) policies (Brown and Korff 2009: 125).

Another way of overcoming the boundaries between the core agencies in the control and security domain is subtler yet still more effective. Today the quality of all police work is measured from an intelligence perspective, or as Lemieux (2008) puts it, intelligence-led policing has become the template for all police work. Converging the police and intelligence communities' cultures, guiding value systems and principles of work through joint training programmes can raise levels of trust between agencies and thus foster the confidence necessary for information sharing, but today law enforcement is increasingly driven by 'the idea that all police work, including patrol, should be intelligence led... [And this is] causing a "minor revolution"' (Lemieux 2008: 163).

Information sharing and exchange

Information sharing and exchange does not in itself blur the institutional barriers between agencies, but the nature of the large-scale information sharing activities being carried out does shed new light on the position of intelligence activities in the law enforcement domain. The resources spent on and the knowledge developed by such large-scale information gathering and analysis is de facto changing police officers into intelligence actors or intelligence material users. It would be too contentious to claim that the right to be free of unwarranted surveillance by law enforcement agencies is being directly jeopardised. The information exchange being carried out by large-scale EU information management systems (e.g. SIS II, VIS, EURODAC, API, ECRIS, PNR etc.)⁶ is regularly facilitated horizontally, i.e. only *among* police personnel. But the large-scale cross-border information management is causing the cultural borders between law enforcement and intelligence communities to disappear.

Some EU initiatives are having a direct impact on the functional borders among agencies in the control and security domains. At the end of May 2004, the European Commission issued a Communication to the Council of Europe and the European Parliament the aim of which was enhancing access to information by law enforcement agencies - EU information policy (European Commission 2004). This would then facilitate the free movement of information between the competent authorities of the member states. The

Commission claimed: 'Compartmentalisation of information and lack of a clear policy on information channels hinder information exchange' (European Commission 2004: 3). The final goal of the Commission set forth in the document was ambitious: it proposed introducing intelligence-led law enforcement at local, national and European levels.

The pro-active agenda advocated in the Communication aimed precisely at overcoming barriers between the law enforcement and intelligence communities. The intention of the Commission is to improve information exchange

not only between police authorities, but also between customs authorities, financial intelligence units, the interaction with the judiciary and public prosecution services, and all other public bodies that participate in the process that ranges from the early detection of security threats and criminal offences to the conviction and punishment of perpetrators (European Commission 2004: 4).

To paraphrase Haggerty and Ericson's notion of 'rhizomatic surveillance' (2000), such 'rhizomatic data-sharing' blurs the functional boundaries between agencies even further.

The European Criminal Intelligence Model (ECIM), the construction of which the Commission set in motion with the Communication, is further supported by a set of minimum standards for national criminal intelligence systems. The latter should enable compatible threat assessments at the European level and be based on comparable core elements for effective access, collection, storage, analysis and exchange of data and information. The Commission claims, amongst other things, that intelligence agencies could and should play an important role in the fight against crime and that police work and judicial activity should both rely more on intelligence. In other words, the ECIM is a policing plan for co-ordinating the investigation of organised crime throughout the EU, a plan based on a method of 'intelligence-led policing' (cf. Brady 2007: 17).

Another instrument for the regulation adopted at the EU level for collating, analysing and enhancing information from intelligence and police services is a special Counter-Terrorism Task Force established within Europol. The Task Force was re-established as a separate entity after the terrorist bombings in Madrid. This specialised unit consists of terrorism experts and liaison officers from police and intelligence services of the EU member states. Its brief is to collect all relevant information and intelligence concerning the current threat of terrorism in the European Union; analyse the collected information and undertake operational and strategic analysis; and formulate threat assessments, including targets, modus operandi, and security consequences.

While Europol is very protective of the role it takes in specific cases, it is difficult to assess the blurring taking place at the EU level. The concrete accomplishments achieved through liaisons between agencies are often achieved by European counter-terrorism officials meeting separately from EU Ministers. Deflem (2006: 346) reports how several meetings of police and intelligence officials were held ('EU Police chiefs') to discuss the Madrid attacks immediately after the bombings there in 2004. In Dublin, the European Chiefs of Police Task Force, representing all 25 (then current and future) EU states, held a two day conference with representatives of Europol, Interpol, and police officials of Norway and Iceland. Coinciding with the police meeting was an additional meeting of intelligence chiefs from five European nations (Britain, France, Germany, Italy and Spain) in Madrid. Similarly, a few days after the 7 July bombings in London, a confidential meeting of police, intelligence officials and forensic experts was held at Scotland Yard.

There are two other important documents with regard to information sharing and exchange at the EU level. First, there is the Hague Programme (European Council 2004), which sets out the principle of availability of information and access to information and invokes the goal of setting up and implementing a methodology for intelligence-led law enforcement to follow at EU level. Second, there is the Treaty of Prüm (Council of the

European Union 2005), also referred to as the Prüm Convention or the Schengen III Agreement from 2005, adopted outside the EU framework and later subsumed into the provisions of EU law for police and judicial cooperation by Council Decision 2008/615/JHA (Council of the European Union 2008).⁷ The Treaty of Prüm implements the Hague programme. Its objective is the 'further development of European cooperation, to play a pioneering role in establishing the highest possible standard of cooperation especially by means of exchange of information' (Council of the European Union 2005: 3). Further developments at the EU level are expected from the new European Information Exchange Model in 2012 as indicated in the Commission's Stockholm Programme Action Plan (European Commission 2010).

The question that arises at this stage is why the proximity of the agencies discussed here should be viewed as problematic in the first place. I have claimed throughout this article that the ever-closer relationship between police and intelligence agencies undermines the right to a fair trial. Information gathered by intelligence agencies typically reveals concrete actions by definite individuals. Should such information be used only to shape policy-makers' decisions and set overall policies, or should it be used to prosecute actual suspects? There is no straightforward and general answer to this question. But some countries such as the USA and Slovenia have set up special balancing procedures for cases where the interests of the state in pursuing security collide with individual human rights. Because Slovenia is a member state of the Council of Europe, the concern now will be to gain an overview of the European Court of Human Rights' decisions regarding such balancing procedures.

LIMITING THE USE OF INTELLIGENCE DATA IN CRIMINAL PROCEDURE

Information gathered by intelligence services can be used in criminal proceedings in several ways (Vervaele 2005: 3, 24). First, such information can be used as a lead for initiating criminal investigations. This is unanimously regarded as the least problematic issue. Second, intelligence information may give rise to reasonable suspicion or another standard of proof or form a sufficient basis for the use of coercive measures sanctioned under criminal law. Such use of intelligence can be regarded as information laundering (Vervaele 2005: 25), since the information concerned is issued by a different body to the one which first gathered it and is wrapped in the veil of 'confidential sources'. Third, there is the use of information *directly* provided by intelligence sources as legal evidence in criminal proceedings (through the use of secret evidence in *ex parte* procedures). This is the issue that provokes the most intense debate. As with the second type of usage, information used directly in this third manner is subject to no legal check before it is collected, and subsequently acquires the status of legal evidence without any safeguards.

Limiting the use of intelligence in the U.S.

The foundations for regulating intelligence and establishing its legally non-binding nature can be traced as far back as the writings of the American Founding Fathers. Thomas Jefferson wrote to a friend:

A strict observance of the written laws is doubtless one of the high duties of a good citizen, but it is not the highest. The laws of necessity, of self-preservation, of saving our country, by a scrupulous adherence to written law, would be to lose the law itself, with life, liberty, property and all those who are enjoying them with us: thus absurdly sacrificing the end to the means (Manget 2007).

In other words, intelligence was always supposed to be governed by a law of self-preservation that stands above the written (state-imposed) law. The sense that the law

of self-preservation governed secret intelligence activities, as Jefferson explained, added to the Federal Judiciary's reluctance to exert its jurisdiction in such areas (Manget 2007).

This reluctance to regulate intelligence activities began to dwindle later in the 1970s, prompted by a number of cases in which intelligence deviated from its traditional role. The activities of the executive branch at this time came under growing scrutiny from the press, the public, Congress and the Federal Judiciary. Since then judges have fashioned their own procedures to balance the competing interests of the state and those of an individual falling under the state's gaze (Manget 2007).

The Classified Information Procedures Act (CIPA) passed in 1980 began regulating the use of intelligence and defined a procedure for balancing government's right not to disclose evidence against a suspect with the suspect's right to a fair trial. In order to avoid previous ad hoc treatments of the issue, the CIPA's procedure set the conditions under which classified information can be reviewed by means of regular criminal procedures for establishing the discovery and admissibility of evidence before the said information is publicly disclosed. Judges were allowed to determine issues presented to them both in camera (in chambers) and ex parte (presented, that is, by only one side, without the presence of the other party). Both interests were thus met. Classified information was revealed to the defendant to the extent necessary to ensure a fair trial and the government was allowed to minimise the quantity of classified information being put at risk of public disclosure by offering unclassified summaries or substitutions for sensitive materials.

Limiting the use of intelligence in Slovenia

Despite the formal separation of law enforcement agencies from the new intelligence agency, the Slovenian Intelligence and Security Agency (SOVA), formally established as an independent agency in April 1989, continued to focus on internal affairs for quite some time after the declaration of independence in the early 1990s. It took two decades for the Constitutional Court of the Republic of Slovenia to rule on a proper minimisation procedure (or so-called 'information-screening wall') in decision Up-412/03 in 2011 (Gorkič and Šugman Stubbs 2010). The Constitutional Court thus finally separated the functioning of the intelligence agency from that of law enforcement.

In the same decision (Up-412/03) the Constitutional Court revealed a secret agreement from 9 September 1993 between the Ministry of Interior (police) and SOVA. The Court was called upon to rule on the constitutional complaint of an appellant who asserted that his right to privacy (vouchsafed by Article 35 of the Constitution of the Republic of Slovenia) and privacy of correspondence and other means of communication (Article 35 of the Constitution of the Republic of Slovenia) had been violated by SOVA's execution of secret surveillance. The appellant was suspected of drug trafficking and a court ordered that secret surveillance of his telecommunications be carried out. Legally, the monitoring of electronic communications by the use of listening and recording devices must be implemented by the police, according to an explicit provision of the Criminal Procedure Act (then § 2 and now § 5, Article 152 of the Criminal Procedure Act). However, according to the secret agreement, SOVA was authorised to carry out monitoring instead of the police, because the police 'was not in possession of listening and recording devices'. The police, noted the Constitutional Court, is 'the competent agency in a democratic society vested with powers to prevent and repress crime including the legitimate use of force' (§ 13 of the Up-412/03 decision). By defining the agency authorised to execute an order (an investigating judge) and the form of an order (written), the legislator indicated that not only the ordering phase, but also the executing phase is of great importance. The Constitutional Court held that the appellant's right to privacy and privacy of correspondence and other means of

communication had been violated. The records gathered by the intelligence agency were thus to be excluded from the new trial.

The Constitutional Court made another groundbreaking ruling effecting the proximity between law enforcement and intelligence in Slovenia with decision U-I-271/08 from 24 March 2011, which stipulated that confidential evidence may be concealed from the defence for three reasons: when national security is concerned; when witnesses at risk of reprisals need to be protected; or, when police investigation methods need to be kept secret. The minimisation procedure contested before the Court was the following: when the police wished to conceal evidence for the above reasons, the defence could request that the Minister of the Interior relieve a police agent or other individual assisting the police of their duty to keep information secret (Article 56 of the Police Act). However, the Constitutional Court held that such a minimisation procedure would violate the defendant's right to judicial protection, which provides everyone with the right to have any decision regarding his or her rights, duties and any charges brought against him or her made by an independent, impartial court as constituted by law (Article 23 of the Constitution of the Republic of Slovenia).

The Court nevertheless admitted that the equality of arms does not require a complete disclosure either of incriminating evidence or indeed evidence benefiting a defendant. The rights of the defence are not absolute and evidence may be kept secret in special circumstances, if such a measure is necessary and proportionate, stipulated the Court. But the Court also ruled that when immunity is claimed for a document in the public interest, it is for the court to decide whether the claim should be upheld or not. The regulation that vested such powers in the Minister of the Interior thus also violated the defendant's right to defend him or herself.

The Court outlined the proper minimisation procedure to be followed until the Police act is amended: when the prosecution claims public interest immunity for evidence and the Minister of the Interior does not relieve a police agent or other person of their duty to keep information secret, the Minister must inform the president of the Court of Appeal about the situation, providing an explanation and his decision. The president of the Court of Appeal must then trigger an *ex parte* procedure and notify the defence that the procedure has begun. The minimisation procedure remains adversarial only to the extent permitted by the nature of the concealed evidence. The president of the Court of Appeal makes a decision after an *in camera* hearing and the decision is final.

The use of intelligence in the ECtHR case law

The European Court of Human Rights (ECtHR) has ruled on the use of intelligence information in criminal proceedings in cases involving the use of evidence provided by anonymous witnesses, undercover agents, informants and agents provocateurs. The court's case law unveils the growing intelligence powers discernible in 'regular' criminal procedure and a permanent threat to the rights to liberty (Article 5 of the Convention for the Protection of Human Rights and Fundamental Freedoms; ECHR) and a fair trial (Article 6 ECHR).

Regarding the second manner in which information gathered by intelligence agencies is used in criminal proceedings, that is when intelligence information forms a sufficient basis for the use of coercive measures under criminal law, the ECtHR admitted in *Fox, Campbell and Hartley v. UK* (1990) that in the case of terrorism intelligence is often used that may not be made public, not even in a court of law, without endangering the source. The central question in the case was whether authorities must disclose information, and if so, *which* information in order to enable a test of the lawfulness of the arrest in the event that it was based on confidential intelligence. The court concluded that 'the respondent Government has to furnish at least some facts or information

capable of satisfying the Court that the arrested person was reasonably suspected of having committed the alleged offence'. It subsequently decided that there had been a violation of Article 5(1)(c) of the ECHR.

The other question that emerged before the ECtHR is *who* should perform the balancing act. In *Chahal v. UK* (1996) the ECtHR dealt with the proper procedure to be followed when the prosecution claimed public interest immunity. It emphasised that the balancing exercise must be performed by the judge and not by panels without judicial competence.

The procedure on *how* to balance the right to disclosure of evidence with other interests, such as national security, was tackled in *R. v. Davis, Johnson and Rowe* (1993) (UK) and later by the ECtHR. The Court of Appeal held that it was not necessary in every case for the prosecution to notify the defence when it wished to claim public interest immunity, and outlined three different procedures to be adopted. The first procedure, which must be followed in all cases, stressed the Court, was for the prosecution to give notice to the defence that they were applying for a ruling by the court and indicate to the defence at least the category of the material that they held. The defence would then have the opportunity to make representations to the court. Second, however, where the disclosure of the category of the material in question would in effect reveal information which the prosecution contended should not be disclosed, the prosecution should still notify the defence that an application to the court was to be made, but the category of the material need not be disclosed and the application should be delivered *ex parte*. The third procedure the Court set forward would apply in exceptional cases where revealing even the fact that an *ex parte* application was to be made would in effect disclose the nature of the evidence in question. In such cases the prosecution should apply to the Court *ex parte* without notifying the defence.

This case was brought before the ECtHR because the defence claimed the Court of Appeal should order the prosecution to disclose the name of any person to whom any reward money had been paid for information given to the police. In *Davis and Rowe v. the UK* (2000) ECtHR declared the trial of these appellants to have been unfair and that Article 6 § 1 of the ECHR had been violated. The Court held that English law requires that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused. But the Court also asserted:

... the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security [...], which must be weighed against the rights of the accused. [...] In some cases it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. However, only such measures restricting the rights of the defence which are strictly necessary are permissible under Article 6 § 1 [...] (§ 61 and § 62 of the judgement).

The ECtHR concluded that during the Davis and Rowe trial in the first instance the prosecution had decided, without notifying the judge, to withhold certain relevant evidence on grounds of public interest. Such a procedure, whereby the prosecution itself attempts to assess how important concealed information might be to the defence and weigh this against the public interest in keeping the information secret, does not comply with the requirements of Article 6 § 1.

Lastly, in *Edwards and Lewis v. UK* (in 2003; upheld by the Grand Chamber in 2004), the ECtHR ruled on the question raised by the third way in which information gathered by an intelligence agency can be put to use, i.e. whether such information may be used as a legal proof in criminal proceedings. In this case the defence was not informed of the type of evidence involved, since it was obtained by agents provocateurs and the prosecution applied for an *ex parte* procedure, but the material in question was later used as evidence in the trial. Moreover, the undercover police officer concerned was the

only witness called during the hearing and was questioned anonymously. It was thus even more crucial for the defence to be able to verify whether this constituted entrapment by the police. The ECtHR established a violation of Article 6 § 1 of the ECHR.

To conclude, the intelligence services have the task of recognising future or current threats to the democratic legal order and subsequently alerting the competent authorities of these threats. Law enforcement should thus be informed of the outcomes of intelligence operation, although it remains crucial that the secret intelligence information is used in criminal courts only under certain special conditions. Criminal proceedings should include the so-called minimisation procedure, fashioned in a way that both protects sensitive intelligence information and enables the defence to examine incriminating evidence at the same time.

CONCLUSION

Discussion of the boundaries between different actors within the control and security domain is shaped first and foremost by questions of history and place. The cases of USA and Slovenia presented here demonstrate how when both nations gained independence, the paths of intelligence and law enforcement were divided. The intelligence communities then worked in separate fields for years (Best in Sweet 2010: 340) until cross-border crime, growing organised crime and later the sensational terrorist attacks of the early 2000s, or the shifts in perception of the real security threats posed by such attacks, set in motion a process by which the spheres of intelligence and police work drew closer once again.

What has changed today is that law enforcement is becoming more reliant on intelligence and is focusing more on the task of detecting future risks of crime and disorder. The perception that the problems of terrorism, organised crime, cybercrime, human trafficking and other forms of serious crimes threaten the very foundations of democratic nation states has encouraged or excused moves to close the gap between agencies in the control and security domain. These threats, whether perceived or real, made law enforcement officers not only the first responders but also first preventers of crime and disorder. These changes expanded the role of intelligence and led to an enhanced policing capacity. They facilitated the exchange of information between law enforcement agencies and the intelligence community. They triggered the formation of new hybrid organisations. They merged police and intelligence cultures. They raised special far-reaching 'omnibus' legislation. And finally, they pushed information gathered by intelligence services for use into criminal proceedings. This last development involved by-passing fundamental criminal procedure rights (such as the right to a fair trial) in all jurisdictions which have not installed a special minimisation procedure to balance the rights of the government with the defendant's right to due process of law. It may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest (e.g. not to compromise a source of intelligence or disclose the methods and means of police work). Despite these developments, the article argues that these balancing acts between defendants' right to a fair trial and public interests should be performed by an independent judicial body. Categorisations such as police, intelligence or military should thus remain distinct and discrete regardless of the undoubted facts that the security actors themselves are 'only human', and that in practice their work overlaps and requires a great deal of communication and co-operation: those facts provide the very reason why criminal proceedings should be protected by keeping the official and legal lines between intelligence and law enforcement as absolute as possible.

The article does not tackle other equally important boundaries in the control and security domain, especially not the process of privatisation of intelligence activities. With the deepening of the financial crisis in Europe member states are forced to outsource their

security-related tasks to the 'free market' and to delegate them to the European level. But private companies are not as intensely regulated as states when conducting intrusive, for instance, surveillance measures for their clients. And the same could be said for the EU institutions. The biggest threat to civil liberties should be expected to come from private and not public security agencies in the future. Future research should also analyse other negative aspects of blurring boundaries between the two selected security actors, not only the information laundering effect. Lastly, it would be of great benefit if future research would also tackle the positive outcomes of blurring boundaries, such as the trend towards increased regulation of intelligence agencies. This was only briefly mentioned in the article, but deserves an in-depth elaboration on its own.

ACKNOWLEDGEMENTS

I am indebted to the Research Council of Norway for the Yggdrasil fellowship in 2012 that facilitated this article. I would like to record my gratitude also to the members of the Working Group 4 Public Policy and the Regulation of Surveillance of the COST Action IS0807 'Living in Surveillance Societies' for providing comments on an earlier draft of the paper and the anonymous reviewers and editors for helpful suggestions on improving the article. I feel very much obliged to John Stubbs, who completed the line editing that far surpasses the usual work of an editor.

¹ The Bundestrojaner ('Federal Trojan') affair in Germany, for instance, exposed the possibilities of Federal Police malware.

² The New York Police Department is supposed to be launching a 'Domain Awareness' computer system that links existing police databases with live video feeds, including cameras using vehicle license plate recognition software.

³ New proposal for the Act on Police Organisation and Work (ZODP) from September 2012. More at www.dnevnik.si/novice/slovenija/1042550385, accessed 12 August 2012.

⁴ PATRIOT is an acronym for 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001'.

⁵ Similar far-reaching amending legislation was adopted in Germany, where The Counter-Terrorism Act significantly improved the sharing of information between authorities by amending at least 14 laws.

More at http://www.bmi.bund.de/EN/Themen/Sicherheit/Terrorismus/SichBehoerden/SichBehoerden_node.html, accessed 16 August 2012.

⁶ See the Communication from the Commission to the European Parliament and the European Council, Overview of information management in the area of freedom, security and justice (COM(2010)385 final, 20 July 2010).

⁷ The European Council's Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

REFERENCES

- Andreas, P. and Price, R. (2001). 'From War Fighting to Crime Fighting: Transforming the American National Security State', *International Studies Review*, 3 (3): pp. 31-52.
- Bayley, D.H. and Shearing, C. (2001). *The New Structure of Policing: Description, Conceptualization and Research Agenda*. Washington, DC: National Institute of Justice.
- Bigo, D. (2005). *Les nouveaux enjeux de l'(in)sécurité en Europe: terrorisme, guerre, sécurité intérieure, sécurité extérieure*. Paris: L'Harmattan.
- Bigo, D. (2000). 'When Two become One: Internal and External Securitisations in Europe', in M. Kelstrup and M.C. Williams (eds), *International Relations Theory and the Politics of European Integration, Power, Security and Community*. London: Routledge: pp.320-360.
- Bolfek, B. (2010). *Teritorialna obramba kot oblika vojaške organizacije*. Master thesis. Ljubljana: Univerza v Ljubljani. Available at URL: http://dk.fdv.uni-lj.si/magistrska_dela_2/pdfs/mb22_bolfek-boris.pdf [Accessed 15 October 2011].
- Brady, H. (2007). 'Europol and the European Criminal Intelligence Model: A Non-state Response to Organised Crime', ARI 126. 1.12.2007. Available at URL: http://www.realinstitutoelcano.org/analisis/ARI2007/ARI126-2007_Brady_EUROPOL.pdf [Accessed 5 November 2011].
- Broesder, W.; Vogelaar, A.; Euwema, M.; op den Buijs, T. (2010). 'The Peacekeeping Warrior: A Theoretical Model', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. V. Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.171-184.
- Brown, I. and Korff, D. (2009). 'Terrorism and the Proportionality of Internet Surveillance', *European Journal of Criminology*, 6 (2): pp. 119-134.
- Cole, D. and Lobel, J. (2007). *Less Safe, Less Free: Why We Are Losing the War on Terror*. New York: New Press.
- Council of the European Union (2008). *Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*.
- Council of the European Union (2005). *Prüm Convention*, adopted 27 May 2005, available at: <http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf> [Accessed March 17, 2012].
- Crawford, A.; Lister, S.; Blackburn, S.; Burnett, J. (2005). *Plural policing: the mixed economy of visible patrols in England and Wales*. Bristol: Policy Press.
- De Weger, M. (2010). 'Striving for Symmetry: Constabularisation, Security and Security Complexes', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. V. Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.111-126.
- Deflem, M. (2006). 'Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective', *Justice Quarterly*, 23 (3): pp. 336-359.
- den Boer, M.; Janssens, J.; Beken, T.V.; Easton, M.; and Moelker, R. (2010). 'Epilogue: Concluding Notes on the Convergence between Military and Police Roles', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. V. Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.223-228.
- Easton, M.; den Boer, M.; Janssens, J.; Moelker, R.; Vander Beken, T. (2010) (eds). *Blurring Military and Police Roles*. The Hague: Eleven International Publishing.
- Easton, M. and Moelker, R. (2010). 'Police and Military: Two Worlds Apart?', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. V. Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.11-32.
- European Commission (2010). *Action Plan Implementing Stockholm Programme*, COM (2010)171 final, 20 April 2010.

European Commission (2004). *Communication from the Commission to the Council and the European Parliament. Towards enhancing access to information by law enforcement agencies (EU information policy)*, COM/2004/0429 final from 16 June 2004.

European Council (2004). *The Hague Programme: Strengthening Freedom, Security and Justice in the European Union*, adopted 5 November 2004, Official Journal of the European Union, C 53/1, 3 March 2005.

Ganser, D. (2005). *NATO's Secret Armies: Operation GLADIO and Terrorism in Western Europe*. London, New York: Frank Cass.

Gorkič, P. and Šugman Stubbs, K. (2010). *Praktikum za kazensko procesno pravo: odločbe in mnenja*. Ljubljana: GV založba.

Haggerty, K. D. and Ericson, R. V. (2000). 'The surveillant assemblage', *British Journal of Sociology*, 51 (4): pp. 605-622.

Janssens, J. (2010). 'Blur the Boundaries! Policing in Contemporary Peace Operations', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. V. Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.79-110.

Jauregui, B. (2010). 'Civilised Coercion, Militarised Law and Order: Security in Colonial South Asia and the Blue in Green Global Order', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. Vander Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.57-77.

Klerks, P. (1993). 'Security Services in the EC and EFTA countries', in T. Bunyan (ed), *Statewatching in the New Europe: A Handbook on the European State*. Nottingham: Russell Press: p.66.

Kraska, P.B. (2007). 'Militarization and Policing – its relevance to 21st century police', *Policing*, 1 (4): pp. 501-513.

Kraska, P.B. (1996). 'Enjoying militarism: political/personal dilemmas in studying U.S. police paramilitary units', *Justice Quarterly*, 13 (3): pp. 405-429.

Last, D. (2010). 'Blending through International Development. Police and Military Roles in Peacekeeping and Stabilisation Operation', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. Vander Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.33-56.

Lemieux, F. (2008). 'Information technology and criminal intelligence: a comparative perspective', in S. Leman-Langlois (ed), *Technocrime. Technology, crime and social control*. Cullompton: Willan Publishing, pp.139-168.

Lemieux, F. and Dupont, B. (eds). (2005). *La militarization des appareils policiers*. Presses de l'Université Laval.

Loader, I. (2002). 'Policing, Securitization and Democratization in Europe', *Criminal Justice*, 2 (2): pp. 125-153.

Loader, I. (2000). 'Plural policing and democratic governance', *Social and Legal Studies*, 9 (3): pp. 323-345.

Lutterbeck, D. (2005). 'Blurring the Dividing Line: The Convergence of Internal and External Security in Western Europe', *European Security*, 14 (2): pp. 231-253.

Manget, F. F. (2007). 'Intelligence and the Rise of Judicial Intervention. Another System of Oversight', Available at URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/manget.htm#top> [Accessed 24 August 2012].

Neuteboom, P. (2010). 'Constabulary Force: A Viable Solution to Close the Security Gap?', in M. Easton, M. den Boer, J. Janssens, R. Moelker and T. Vander Beken (eds), *Blurring Military and Police Roles*. The Hague: Eleven International Publishing: pp.136-155.

O'Neill, M., Léonard, S., Kaunert, C. (2011). 'Introduction: Developments in European Security', *Journal of Contemporary European Research*, 7 (4): pp. 431-434.

Pirjevec, J. (2011). *Tito in tovariši*. Ljubljana: Cankarjeva založba.

Pusić, E. (1985). *Upravni sistemi*. Zagreb: Grafički zavod Hrvatske.

SOVA Act (2006). Slovene Intelligence and Security Agency Act, *Official Gazette of the Republic of Slovenia*, No. 81/2006-UPB2.

Svendsen, A. D. M. (2011). 'On 'a Continuum with Expansion'? Intelligence Co-operation in Europe in the Early Twenty-first Century', *Journal of Contemporary European Research*, 7 (4): pp. 520-538.

Sweet, K. M. (2010). 'Information Sharing between Police and Intelligence Agencies', in G. Cordner, A. Cordner, D.K. Das (eds), *Urbanization, Policing and Security: Global Perspectives*. Boca Raton, London, New York: CRC Press: pp.339-352.

Vervaele, J. (2005). 'Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?', *Utrecht Law Review* 1 (1): pp. 1-27.

Wakefield, A. (2005). 'The Public Surveillance Functions of Private Security', *Surveillance & Society*, 2 (4): pp. 529-545.

Završnik, A. (2012). 'Transformations of Surveillance: from National Security to Private Security Industry', in A. Šelih, A. Završnik (eds), *Crime and transition in Central and Eastern Europe*. New York: Springer: pp.67-96.

Zedner, L. (2007). 'Pre-crime and post-criminology?', *Theoretical Criminology*, 11 (2): pp. 261-281.