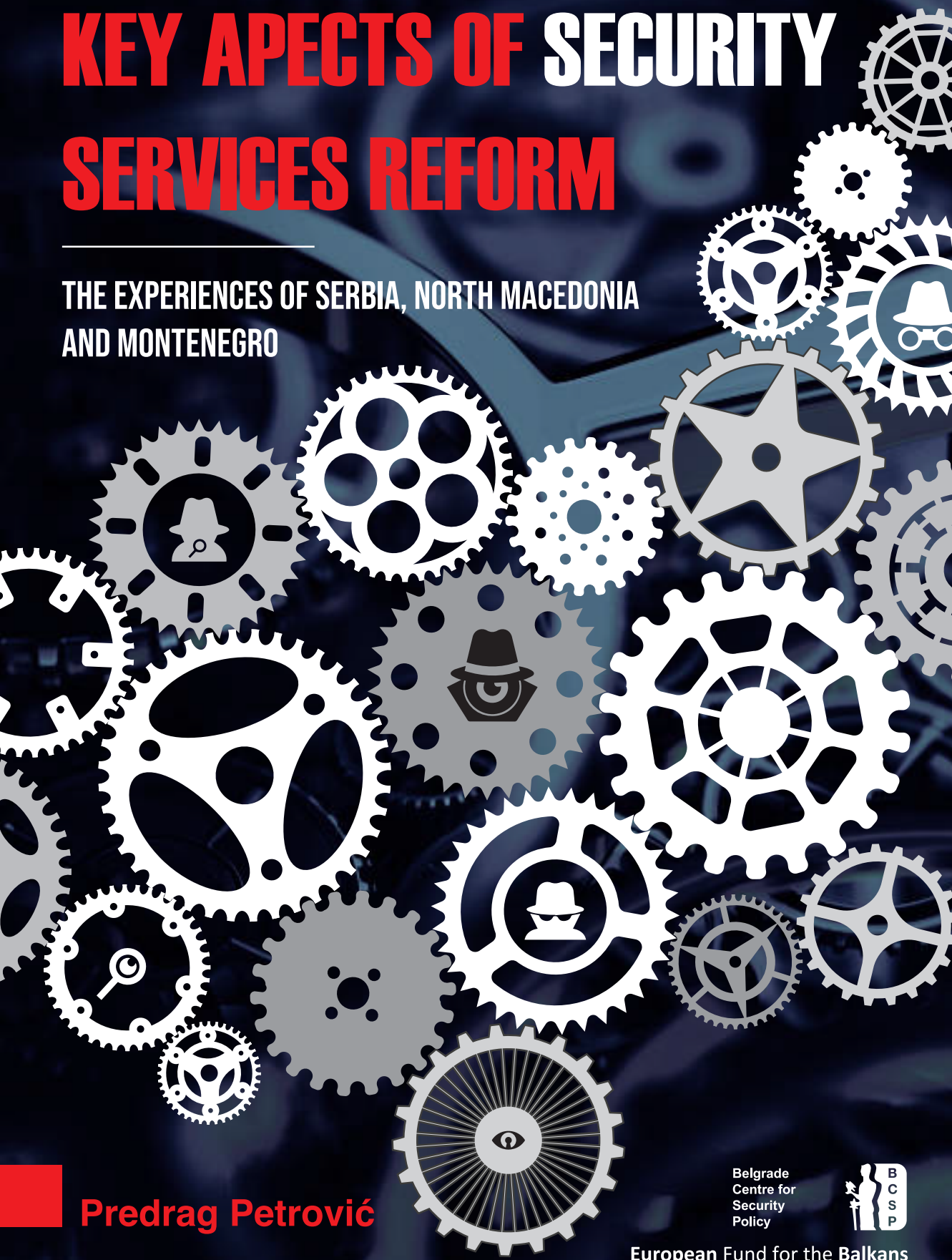
KEY APECTS OF SECURITY SERVICES REFORM

THE EXPERIENCES OF SERBIA, NORTH MACEDONIA AND MONTENEGRO



Predrag Petrović

Belgrade Centre for Security Policy

BCSP

European Fund for the Balkans

KEY ASPECTS OF SECURITY SERVICES REFORM

The Experiences of Serbia, North Macedonia and Montenegro

Publisher:

Belgrade Centre for Security Policy

Đure Jakšića 6/5, Belgrade

Tel. +381 (0)11 328 72 26

office@bezbednost.org

www.bezbednost.org

Author:

Predrag Petrović

Design and Pre-Print:

DTP Studio

Belgrade, January 2020.

European Fund for the **Balkans**

The Policy Brief began as part of the “Who Oversees the Overseers: Western Balkan Security Services” project, which is supported by the European Fund for the Balkans (EFB). The content of this study is the exclusively responsibility of its author and it in no way reflects the views of the EFB.

CONTENTS

Introduction

Security services derive their power from secret and exclusive access to and control of information, on the basis of which they covertly influence the most important decisions and processes in the state and in society. This is why any reform of the security services must entail the establishment of institutional arrangements such as mechanisms and procedures that prevent the abuse of covert data collection and make effective oversight and control possible. In order for reform of the security services to be successful, however, it is not enough to simply design mechanisms and procedures in accordance with democratic standards – it is also necessary to comprehensively reform human resources in the services as existing employees are precisely the people who are unlikely to comply with the new norms. Over the following pages we will show in detail how to regulate covert surveillance of communications and the human resources of the security services in a manner that would reduce the likelihood of (personal and political) abuses. These two key segments of security service reform are the focal point of this study. The conclusions and recommendations we make here are based on the findings of research conducted into the security services of North Macedonia, Serbia and Montenegro and that are presented in publications referenced at the end of this text.

Recommendations

a. Covert Surveillance of Communications

- A special operational and technical body should be formed to act as an independent mediator between the courts, as the bodies that order covert surveillance of communications, and the security services, as the bodies that execute it.
- It is very important to ensure that mobile equipment used for covert surveillance of communications is used only upon receipt of court approval, that each use of such equipment is indelibly recorded and that such equipment is stored in such a way that only authorised personnel can access it.
- For the purposes of effective control, it is necessary to maintain separate and comparable records of each and every instance in which equipment for covert surveillance of communications is accessed.

b. Human Resource Management

- The criteria and procedures for candidate selection for senior positions in the security services (the directors and deputy directors) should be regulated by law and their term in office and the scope of their powers should be defined.

- Effective reform of the security services requires the overhaul of human resources, which entails the release of personnel socialised in the secret services of previous, undemocratic regimes.
- The European Union should pay more attention to the security and intelligence sectors in the accession process of Western Balkan countries, given the great potential for the abuse of this sector for the purposes of state capture.

Covert Surveillance of Communications

Formation of an Operational and Technical Centre as an Independent Mediation Body

One of the ways in which it is possible to improve oversight and control of the security and intelligence agencies and police is to detach equipment for covert surveillance of communications from these actors and entrust it to a dedicated institution. This would be achieved by forming a separate body (an operational and technical agency or centre), which would be independent of the security services and the police and which would physically house all of the equipment for covert interception of communications. The main task of this institution would be the activation and management of measures for covert surveillance of communications. In practice this would mean that, upon receiving judicial approval for the use of measures for covert surveillance of communications, the security services and police would not be able to independently activate and manage these measures but would instead have to rely on a separate institution for their activation and implementation.

Viewed in greater detail, the process of approving and implementing the measures would look like this (see figure). The security services would compile a proposal for the use of measures for covert surveillance of communications, which they would then submit to the competent court. The court would then assess whether all of the legal requirements, whether formal or substantive (the existence of grounds for suspicion, the principles of necessity and proportionality), have been met. If the outcome of this assessment is positive, the court would then issue an order to implement the measures. It is important to note here that the court drafts two documents with different levels of data and information:

1. A document that is passed to the security services; this would contain all of the details pertaining to the covert surveillance of communications, such as, for example: the identity of the person targeted by the measure, their telephone number, how long the measure can be implemented, the grounds for suspicion and an explanation of why the measure is necessary.

2. A document that is passed to the institution that activates and manages the implementation of the covert surveillance of communications; this would contain only the data necessary for the measure to be implemented (e.g. the telephone number and the timeframe for the implementation of the measure).

Some security and information technology professionals believe that it is possible to go a step further and to make the implementation of the measure completely anonymous through, for example, the mediating institution receiving a document with a barcode that would automatically activate the measure when scanned. In this way, this institution would have no way of knowing which numbers are targeted for surveillance.

Upon receiving a court order, the operational and technical agency would activate the implementation of the measure – i.e. ensure that the security service or police have access to the results of the surveillance or the content thereof. The advantages of this approach are that, on the one hand, the security services cannot implement these measures independently even when they have judicial approval to do so as the technical capabilities for this have been transferred to a separate agency. On the other hand, the operational and technical agency has very limited insight to the data that determines who is targeted by the measure and no insight at all into the content of data gathered. This would, therefore, introduce an additional level of checks and balances to the implementation of these measures, which would make the abuse thereof more difficult.

An additional barrier to misuse would stem from the fact that the director of the operational and technical agency would be appointed by and answerable to the executive branch, usually the government, with prior approval or consent from other security and intelligence sector actors. Moreover, the conditions for dismissal of directors would be very strict in order to minimise the likelihood of their discretionary dismissal.

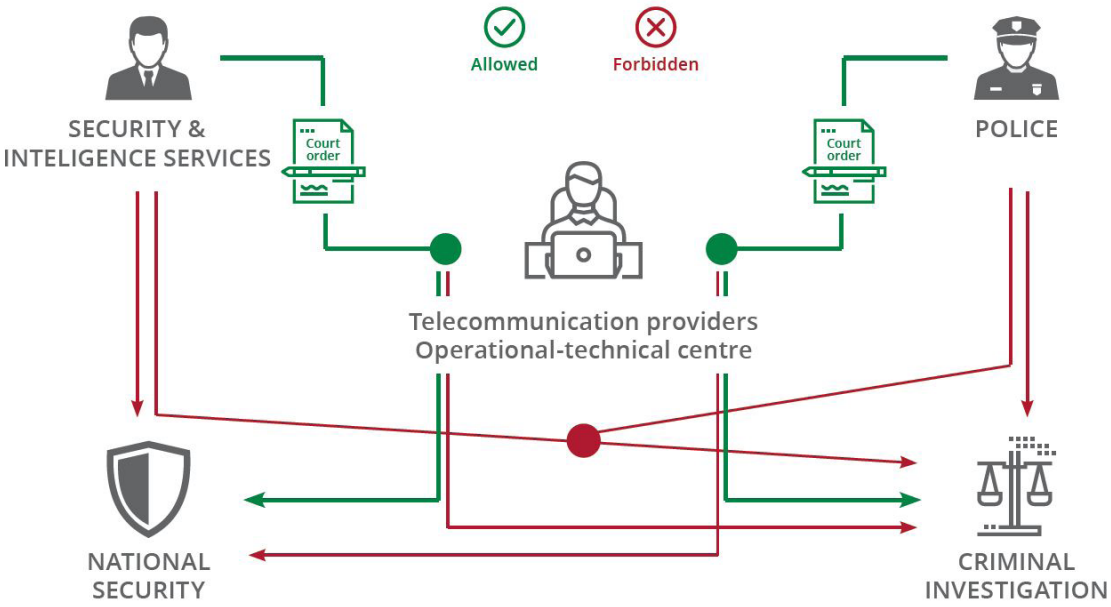


Figure: The role of the operational and technical centre in covert surveillance of communications

Mobile Equipment for Covert Surveillance of Communications

With the emergence and development of (mobile) telecommunications devices and infrastructure, devices for the interception of mobile communications were also developed. For example, the famous Stingray Catcher surveillance system, which enables a mobile device to mimic a mobile telephony base station and forces nearby mobile phones to connect to it, rather than to the real base station. This in turn enables the conversation to be monitored. Also in widespread use are devices for covert surveillance of mobile telecommunications via wireless internet (Wi-Fi interception systems), which work on similar principles.

Mobile devices for communications interception do make the work of the security services easier but they also enable numerous abuses and the unrestricted violation of human rights, as is illustrated by cases from both the Western Balkans and from developed Western countries. There has, as a result, recently been a focus on ways to monitor and control mobile surveillance equipment. This can be achieved by storing this equipment in such a way that it can only be accessed by authorised personnel. The equipment would then be used only when this has been approved by a court and each use of the equipment would be recorded.

There are a number of models for the storage of this kind of equipment. The first of these is to entrust the equipment to a separate operational and technical agency. The second approach is to locate the equipment at the security services and the police. All other approaches are a combination of these two. For example, mobile equipment for

covert surveillance of communications used to gather data for criminal proceedings would be entrusted to public prosecutors' offices, while equipment used for national security purposes would be in the possession of the security services or the operational and technical agency. Of course, this could give rise to disputes between the security services and the police over "ownership" or "availability" of the mobile equipment at a given time. Additionally, this equipment must be used in close proximity to the target of the surveillance and must, therefore, be deployed evenly across the country.

Whichever model is applied, it is very important to ensure that mobile equipment for covert surveillance of communications is used only upon receipt of court approval, that each use is indelibly recorded and that such equipment is stored in a manner so that it can only be accessed by authorised personnel.

Record-Keeping and the Implementation of Covert Surveillance of Communications

Keeping detailed and comprehensive records of the implementation of covert surveillance measures is essential for their effective oversight and control. This implies keeping records on the number of times such measures were proposed, as well as the number of times these measures were approved and rejected. Record-keeping should also facilitate the classification of measures by type, as well as by the reason they were applied (extremism, terrorism, corruption, etc.). If the security services have the power to apply covert surveillance measures in order to gather evidence for criminal proceedings, the records should also reflect for which offences the measures were applied and the outcome of their use. In the United States, these records also state how much the measures cost, in order to make it possible to assess, through cross-referencing with other criteria, whether their implementation was expedient.

It is not, however, enough for such records to be kept only by the security services themselves, they must be also be maintained by the judiciary, by other relevant governmental institutions (e.g. institutions responsible for protecting personal data), and by telecommunications and internet providers. The records of the latter actors must record each intercept, whether it was conducted at the request of the telecommunications and internet providers or whether it was conducted by the security services directly. Furthermore, it is important to ensure technical conditions are in place to prevent the records from being tampered with at a later date. Outdated, inconsistent and poorly maintained records – or even the absence of proper records – as well as the possibility of records being tampered with were identified as serious concerns by the Ombudsman and the Commissioner for Information of Public Importance when conducting oversight and control of the security services and telecommunications providers in Serbia.

Well-kept and up-to-date records maintained by all of the actors that approve and implement covert surveillance measures are a basis for effective oversight as they

make it possible for data held by various actors to be compared and cross-referenced. As the Serbian Commissioner once noted, in the absence of this, "the services have to be taken at their word".

Human Resources

Passing the best possible legislation, norms, rules and procedures, all aligned with the most modern democratic standards will not much alter how the security services go about their business if they continue to be staffed by personnel accustomed to circumnavigating or breaking rules and regulations. The backbone of every institution are its employees because how they act (in accordance with the law or counter to it) shapes the institution to which they belong. This is why fundamental institutional reform must also encompass human resources.

Who Controls the Security Services?

Security services are centralised and hierarchical governmental organisations in which the directors of the services have far-reaching decision-making powers, including (as our research shows) over human resources. It is important here to begin at the top, with the security service directors. As the experiences of Serbia, North Macedonia and Montenegro have shown, the directors have enormous decision-making powers, including over human resources, while the criteria for their appointment and dismissal are not clearly defined.

Since politicisation is a major problem in Western Balkan countries, it is very important to ensure that an individual who has been a member of a political party at any time over the previous five years cannot be appointed as the director of a security service. Moreover, additional checks and balances should be envisaged for the appointment of directors. For example, it should be stipulated that both executive branches (the government and the president) must agree on a candidate and that the parliamentary committee responsible for control of the security services must be consulted prior to their appointment. Increasing the number of institutions whose opinion must be sought prior to the appointment of the director of a security service increases the importance of this office and also reduces the possibility of arbitrary appointments. It is also important to define beforehand the length of the term in office of the director (usually 4-5 years) and whether it is possible for them to be re-selected. So that oversight bodies clearly understand what to scrutinise, it is important to spell out precisely what a director is responsible for. This approach has been adopted in North Macedonia and Montenegro but not in Serbia.

As deputy directors also play a very important role in the management of security services, it is necessary to properly regulate the procedures for their appointment. Comparative practice indicates that the conditions and procedures for the selection

of a deputy director are usually the same as for the director, with the additional requirement that the deputies are put forward by the director. Finally, the criteria for the dismissal of security service directors and their deputies must be clear and the conditions and procedures for this properly regulated.

Who (Still) Works for the Security Services?

The much more difficult task is to reform human resources "in depth" because clear criteria, procedures and instruments must be put in place to determine whether an individual can (continue to) work for the security services. An important role here is played by the selection committee whose task it is to decide, on the basis of established criteria, rules and applied instruments, who is fit to serve in the security services. It goes without saying that the committee must be of a "mixed" type, that is, that it should be composed of experienced security service officers but also of those from "outside", such as human rights experts. In order to ensure the selection committee has the broadest possible support, it is usually stipulated that its members are selected by parliament through a qualified majority, most commonly a two-thirds majority.

The criteria for recruitment are actually a kind of security clearance for security service personnel. In North Macedonia this was attempted through the application of two instruments – an integrity test and polygraph testing. The problem was, however, that these instruments were introduced without first ascertaining the actual state of affairs – for example, polygraph testing could not be implemented because only one working polygraph machine was available. Also potentially problematic is who is responsible for conducting security checks or integrity tests. Are they likely to objectively gather information? It is precisely for this reason that it is important to provide appeal procedures through which security personnel can protect their rights if they feel them to have been threatened.

The case of Montenegro indicates that reform of the human resources of security services is important for the needs and motivations of the country and its society and not because it is demanded by international organisations or foreign states. More specifically, before joining NATO, Montenegro had to "clear out" personnel suspected of having links with Russian security services from the ranks of its National Security Agency (ANB). The legislative underpinning for this was created in 2015 by amending the Law on the National Security Agency and the Law on Pension and Disability Insurance, practically solving this problem by instituting early retirement for around 20 percent of ANB personnel. This ensured Montenegro's NATO membership as other member states no longer had concerns that information exchanged with the ANB would reach a "third party". Although this solved a problem that was important to NATO, it left untouched a series of problems that are important for the people of Montenegro. Principal among them is, of course, the great degree of politicisation

of the ANB. Consequently, any reform of the security services must be thorough and must be driven, shaped and guided by the needs of the parent society, rather than imposed externally.

Sources:

Predrag Petrović, „The anatomy of capturing Serbia's security- Intelligence sector", Belgrade Center for Security Policy, Belgrade, 2020.

Magdalena Lembovski, „More than (de)politicization: The role of security-intelligence service in (de)capturing the state", Eurothink, Skopje, 2020.

Dina Bajramspahić, "An unfinished intelligence sector reform in Montenegro", Institute Alternative, Podgorica, 2020.

About the Author

Predrag Petrović, MPhil, is executive director at the Belgrade Centre for Security Policy, a think-tang of Serbia. He has researched, written, edited, and consulted broadly in issues related to intelligence democratization, privatizing security, (violent)extremism and terrorism, integrity and corruption in the security sector. He has delivered numerous trainings and lectures on oversight of security actors to oversight bodies, faculty students, Western Balkans' think/thanks, and has also contributed to various legislative processes. Petrovic PhD candidate at the Faculty of Political Sciences in Belgrade working on a thesis which explores relationship between democratization and intelligence reform in Serbia.

About the Belgrade Centre for Security Policy

The Belgrade Centre for Security Policy (BCSP) is an independent think-tank dedicated to advancing the security of citizens and society on the basis of democratic principles and respect for human rights. In the focus of the BCSP's interests are all policies aimed at the improvement of human, national, regional, European and global security.

The BCSP supports consolidation of security sector reform and the integration of Western Balkan countries into the Euro-Atlantic community through: research, analysis and policy recommendations, advocacy, education, publishing, expert support for reform and networking between all relevant actors.

Specifically, BCSP probes into the dynamics and achievements of the reform of Serbia's state apparatus of force, as well as the problems of placing this sector under democratic civilian control and oversight.

www.bezbednost.org

About the European Fund for the Balkans

The European Fund for the Balkans is a joint initiative of European foundations that envisions, runs and supports initiatives aimed at strengthening democracy, fostering European integration and affirming the role of the Western Balkans in addressing Europe's emerging challenges.

The up-to-date programme strategy based on three overarching areas – Capacity Development, Policy Development and Regional Cooperation – is channelled via flagship programmes and selected projects, complemented with a set of actions arising from the EFB's regional identity as a relevant player in its fields of focus.

www.balkanfund.org