institut alternativa

National Security Agency and Secret Surveillance Measures - Is there any control?

February 2012.

Summary

In the period between 2005 and 2009, 324 citizens of Montenegro were under SSM undertaken by the NSA, while the data for the last three years is marked as 'secret', and thus unavailable, because their publication would allegedly jeopardize national security.

Surveillance of electronic communication is not precisely defined by law, so it is unclear whether it includes call lists, user locations, IP addresses and alike. Although foreseen as an exception when other measures do not yield results, SSM are applied much more frequently than tracking and surveillance, e.g., five times more frequently in 2008, which requires an explanation of such an approach.

Access to information about the application of SSM is limited in the annual performance reports of the NSA and the Supreme Court. The absence of the procedure and practice of destroying personal data in cases when the basis for continuing the application of SSM has not been determined, as prescribed by law, is worrying.

Judicial control is reduced to the approval of measures and plays no significant role in assessing the application thereof. Interior control of the NSA is not in a position which would allow for efficient and independent oversight. Parliamentary oversight of the SSM application yields poor results. Between 2006 and 2011, the relevant committee: completed only one visit to the NSA; demanded and received one special report about the application of SSM for the period 2008/09; deliberated annual NSA reports containing sporadic and incomplete data on SSM; and rejected one initiative, submitted by a group of opposition MPs, requesting the control hearing of the NSA director. Adoption of the important Law on Parliamentary Oversight of Security and Defense Sector has not stimulated the Committee in terms of overseeing the use of SSM; instead, the Committee was less interested in SSM during 2011 compared to the previous period.

Parlament of Montenegro

Research project was supported by Commission of the Parliament of Montenegro for the Distribution of Funds to Non-governmental Organizations

Introduction

The state needs efficient intelligence and security services with special powers to protect itself from threats to national security and to be more efficient in the fight against organized crime. Secret surveillance measures (hereinafter: SSM) allow the state to act preventively, to detect and to eliminate various forms of threats early. However, apart from being an instrument of protection, they are a powerful lever of the state, susceptible to abuse. Such abuse causes serious damage to the pivotal values of a democratic society which is why continuous control needs to be exercised and oversight mechanisms of its application developed.

SSM applied by the National Security Agency (hereinafter: NSA) include those measures of covert data collection which require higher level of authorization: 1. *surveillance over electronic communication and mail deliveries* approved by the president of the Supreme Court; and 2. *surveillance of facility's interior, closed spaces and objects, with the use of technical means*, approved by the Panel of Judges of the Supreme Court, upon written proposal by the NSA director. Measures are applied when there is a well-founded suspicion of threat to national security. There are three modes of control for applying the measures: judicial, internal and parliamentary control.

By analyzing the legal framework and the application of SSM, the author's goal is to indicate the provisions which are not in line with the standards and best practice in this area, and to identify the possibilities and limits for overseeing the use of these measures at all three levels of control, with an emphasis on parliamentary oversight.

Leading researcher: Dina Bajramspahić

Measure: surveillance over electronic communication?

The Law on NSA[1] stipulates that upon written proposal of the Agency director, the president of the Supreme Court of Montenegro, through his/her decision, approves: *surveillance over electronic communication and mail deliveries* should there exist a well-founded suspicion of threat to national security. This provision is not precisely formulated because the law does not *define what constitutes surveillance over electronic communication and what information about the telecommunication network user is possible to obtain in this manner.*[2]

In other words, from such a formulation stems the assumption that this provision addresses only the content of electronic communication itself, while it remains unknown whether the president of the Supreme Court may also approve the application of secret surveillance over the *telecommunications traffic* (which, for instance, includes call lists). Similarly, it is unclear whether the NSA may seek approval from the president of the Supreme Court to determine the *location of users*; to collect data from *base stations*; and *IP addresses of the internet users*. All the above-mentioned possibilities within the framework of secret surveillance over electronic communication must be at the same level of protection as the contents of phone calls themselves. Such an imprecision leaves room for manoeuvre for NSA's free interpretation and arbitrary application of the measure.

The Law on NSA does not contain a specific provision which would regulate the granting of insight into the information about users' calls. Namely, the law neither defines whether insight into *call lists* is approved by the decision of the president of the Supreme Court, nor does it define the time limit for insight into call lists. Time limitation for insight into call lists is, for example, 3 months in Slovenia, while in Montenegro it is 24 months, assuming that the time limitation related to surveillance over electronic communication is applied to call lists too.

1 *Official Gazette of the RoM, No. 28/05 of 5 May 2005, Official Gazette of MNE, No. 86/09 of 25 December 2009 and No. 20/11 of 5 April 2011.*

2 *For a provision to be considered a law, according to the 'law quality test' of the European Court of Human Rights, it must fulfill the following conditions: 1. Provision must be sufficiently accessible and precisely stated to allow the citizen to base his/her behavior appropriately; 2. Rule must have the necessary forms of predictability and must not allow for unlimited freedom of decision.*

Judicial control

Proposal to apply the measure[3], which the Agency director submits to the president of the Supreme Court / Panel of Judges, does not contain concrete reasons explaining why it is not possible to gather data by applying different methods - methods that are less harmful to the right to privacy and which would meet the requirement of the European Court of Human Rights 'principle of proportionality'.[4] Hence, in practice, surveillance over means of communication is more widespread than the method of tracking and surveillance, even though the Law on NSA foresees the use of surveillance over electronic communication only 'exceptionally'.[5]

Table 2: Number of measures carried out by NSA in 2006, 2007 and 2008

	2006.	2007.	2008.
Method of tracking and surveillance	3 persons	1 person	24 persons
Surveillance over means of communication	91 persons	59 persons	143 persons

In comparative practice, *principle of proportionality* is expressed through a special request stipulated by law. According to this request, proposal for carrying out the measures must include reasons explaining why other measures are inadequate in gathering the relevant data, as well as a statement demonstrating that the application of covert data collection will yield the expected results. This means that at a particular moment of necessity to apply such measures, NSA has quality operative information and indications at its disposal, proving that there is a reasonable ground to suspect that the persons under surveillance threaten national security.

3 *The form of the surveillance proposal (over electronic communication and facility's interior) is defined in Article 15 of the Law on NSA.*

4 *Principle of proportionality, applied in the case of organised crime (Malone vs. UK, 1985), implies proportionality of curtailing human rights and of the purpose of such curtailment. According to this principle, state bodies are obliged achieve their goals with minimal curtailment of human rights or without any curtailment, if possible.*

5 *Article 13 of the Law on NSA*

Procedure for data destruction

Judicial control is reduced to approving the measures. Following the application of SSM, the Law on NSA does not oblige the Agency to deliver the material gathered in this way to the president of the Supreme Court / Panel of Judges for an *assessment of the legality of application*. During this assessment procedure, after the judge's reading, part of the material non-related to the reasons which triggered the use of such measures would be destroyed immediately, as well as other personal data which are irrelevant for security. The rest of the material could then be kept in the records. Such an approach is found in many European countries, of which the experience of Slovenia is the most significant one for Montenegro's security system. In this way, compliance with the constitutional provision on the protection of personal data would be guaranteed. Similarly, compliance with the case-law of the European Court of Human Rights, according to which maintaining *personal* data in secret files embodies the violation of the right to respect privacy, would also be ensured. Destroying previously collected data is further obligatory in case of cessation of reasons urging the continuation of SSM implementation. This issue cannot be a matter of NSA's autonomous decision, without the possibility of control and lacking legal definition.

Informing the citizens

According to the case-law of the European Court of Human Rights, an individual has the *right* to be informed about the use of SSM and about the result of their application in his/her case. This right is also guaranteed to Montenegrin citizens by the Constitution.[6] It is a form of accountability of the institution which applied such measures, and an opportunity for the citizen to take advantage of his/her right to legal remedy.[7] The Law on NSA provides for the possibility of informing the citizen upon his/her own *personal request* about whether personal data of which that individual is the data subject are being processed by the Agency or not. That is an important protection mechanism guaranteeing the respect for the rights of individuals who were under some sort of surveillance by the NSA. However, the possibility of informing the citizens upon their personal request *does not correspond* sufficiently to the constitutional right to privacy for those individuals who are subject to the use of surveillance over electronic communication and facility's interior. Information about the number of persons who have used this right is not available.

Internal control

Internal control of the NSA performance is carried out by the inspector general, accountable to the government. Thanks to his position within the NSA system, he is in possession of the most significant mechanisms for determining illegal application of SSM, via *direct insight into the application itself at the time of application*. He is constantly involved in control process in the areas of: operational affairs, technical affairs, data protection, financial transactions. Still, in '*his work, he has never encountered illegal application of the secret surveillance measures or any other form of abuse*.'[8]

The public character of internal control's work is at the lowest possible level. There is no information about the controls carried out even in a series of problematic cases, involving the work of NSA, which have been known to the public in the previous period. The number of reports on control procedures delivered to the government and NSA director is also unavailable.

Parliamentary oversight

Competencies of the Parliamentary Committee for Security and Defense (hereinafter: the Committee), responsible for overseeing the work of NSA, were prescribed in detail by the Law on Parliamentary Oversight of Security and Defense Sector.[9] This, however, has not stimulated the Committee members to use their authority in overseeing the application

6 *Constitution of Montenegro (Article 43, paragraph 3): 'Everyone shall have the right to be informed about the personal data collected about him or her and the right to court protection in case of abuse.'*

7 *Constitution of Montenegro (Article 20): 'Legal remedy: Everyone shall have the right to legal remedy against the decision ruling on the right or legally based interest thereof.'*

8 *Interview with Vlado Radovic, NSA inspector general, 27 May 2011*

9 *Official Gazette of MNE, No. 80/10 of 31 December 2010*

of SSM. Instead, the Committee was even more inert in this field during 2011. Such a conclusion is based on the fact that during 2011 there were no activities aiming to control the application of measures for covert data collection.[10]

Until now, in terms of oversight of the measures for covert data collection, the Committee performed the following activities:

a) completed one visit to the NSA; requested one special report on SSM[11];
b) discussed annual performance reports of NSA;
c) discussed and rejected one initiative for deciding on a control hearing about the potential abuse of SSM.

a) Visit to the NSA as a control mechanism

Through the initiative taken by the Committee members[12], it has been suggested that the Committee members visit NSA in order to check whether SSM are applied in accordance with the relevant law.[13] Additionally, it has been requested that, even before their visit to the Agency, the NSA deliver to the Committee members a special report on SSM for 2008 and 2009, 'i.e., a review of the use of all such statutory authorities according to the "lines of work" as stipulated by Article 14 of the Law on NSA.'[14] After the report had been delivered, while commending the decision that the Committee members visit the NSA, the Committee member of the opposition party New Serbian Democracy, Goran Danilovic, stated that the report delivered was 'an insult to the MPs', containing only *itemized listing of eavesdropping cases, without providing reasons why such measures were taken*.[15]

During the visit of 12 March 2010, Committee members from the opposition parties refused to enter the NSA building because they had to go through security checks and leave their mobile phones at the entrance[16], so the visit was carried out by the ruling coalition MPs only. Three files were taken as a random sample. In the words of SDP MP, Borislav Banovic: 'In their content, the files followed the legal procedure, they contained justification and the director's request why that was needed, the court's approval, then the actual file, i.e., the material from the secret surveillance itself, then the decision on cessation, or continuation, request for extension if there were grounds for that, in that sense it was good, lawful, thorough and very orderly, but that's what we get at the table.'[17] Simultaneously, he acknowledged that MPs do not have the experience, knowledge or skills to check the data on the application of SSM in detail.

After the visit, MPs notified the public that in 2008 and 2009, the legal procedure was carried out in accordance with the Law on NSA.[18] Written conclusions were not adopted and the Committee did not discuss the visit. MPs did not even use the experience of this one visit sufficiently in order for the 'visit to the institution' as a control mechanism to be used as efficiently as possible in the future control of the NSA work, nor did they use it to gain useful and meaningful information about its work, and specifically, about the application of SSM by the NSA.

b) Annual performance report of the NSA

Discussing the annual performance report is an especially important mechanism of parliamentary oversight allowing the Committee to judge the work of a state body. The precondition is that the report actually provides information about the accomplished work and the achieved results. In the annual performance reports of the NSA, information on the use of SSM

10 Besides discussing the Annual NSA reports for 2010 and 2011, other concrete activities related to the role of the Committee in overseeing the application of SSM, were not even planned - according to the 'Plan for carrying out the oversight role of the Committee for 2011'

11 'Report on the application of method of surveillance over mail deliveries and other communication in 2008 and 2009', March 2010 - marked as secret.

12 Borislav Banovic and Rasko Konjevic (SDP)

13 This initiative, springing from Article 43, paragraph 4 of the Law on NSA, was discussed as item 1 on the agenda of the 14th session of the Committee for Defense and Security, held on 5 February 2010.

14 'Report on the Committee work of the 24th convocation of the Parliament of Montenegro', Podgorica, 3 September 2010

15 Independent Daily 'Vijesti', Politics section (page 3), 2 March 2010

16 Movement and stay in facilities representing security zones of 1st and 2nd degree is defined by provisions stemming from articles 12 and 13 of the Regulation on conditions and way of implementing measures of secret data protection (Official Gazette of MNE, No. 72/08"). All persons with access to secret data, in line with the Information Secrecy Act, are obliged to familiarize themselves with these provisions. Pursuant to article 13, paragraph 2, point 4: 'd) it is prohibited to bring mechanical, electronic and magneto-optic devices, which could be used for illegal recording, taking out or transferring secret information, without authorization.'

17 Interview with MP Borislav Banovic, representative of SPD in the Committee for Defense and Security, 30 May 2011.

18 'Visit to the NSA: Opposition MPs control, but don't like to be controlled', Analitika - information portal, section: Politics-News, 12 March 2010

can be found intermittently[19], and is related only to the number of measures approved.[20] This means that the members of the Committee responsible for the oversight of the use of SSM do not even possess the minimum information about the measures applied by the NSA nor about the results of that application. In contrast to only one numerical information supplied by the NSA, the intelligence agency of Slovenia - SOVA - delivers special reports on the use of SSM every 4 months (and more frequently if requested) to the parliamentary working body, containing a whole set of information as prescribed by the law.

The lack of detailed information limits the Committee in providing an objective assessment of the justification given to apply these measures, and in overseeing the application in general.

Absence of information from the Supreme Court

Annual reports of the Judicial Council on the performance of courts in Montenegro, discussed by the *Committee for political system, judiciary and administration* in parts related to the work of the Supreme Court, does not provide information on SSM. The president of the Supreme Court / Panel of Judges have direct insight into every individual case of measures' application. As such, they can be a useful and important source of information for the Parliament of Montenegro which oversees the work of the NSA and its use of SSM through its relevant working body.[21] Parliamentary oversight of SSM without the information of the Supreme Court on the measures approved/disapproved/extended/ suspended cannot be sufficiently objective.

19 'National Security Agency did not deliver and does not deliver reports on secret surveillance measures. Last year (2010), annual report did not contain information, while previous reports contained only the number of measures taken, from which we cannot draw any conclusions. We can, at the Committee sessions, demand oral report. Essentially, that should be defined by law as compulsory (...) That area of oversight is an empty area when it comes to experience, that area leaves significant room for doubt, that area is indeed partially defined by the Law on parliamentary oversight, but...In the preceding period, less than a year from the Law's adoption, I want to criticize the Committee and all of us, we did not develop the mechanisms of insight into the application of SSM.' Interview with MP Predrag Bulatovic, representative of the Socialist People's Party in the Committee for Security and Defense, 25 May 2011.

20 'During 2006, president of the Supreme Court approved the use of this method in 91 cases.' (2006 NSA performance report) 'In 2007, president of the Supreme Court approved the use of secret surveillance method over mail deliveries and other means of communication for data collection in 59 cases.' (2007 NSA performance report). Performance reports of the NSA for 2008 and 2009 are marked as 'secret' in their entirety. The 2010 report, in parts other than those marked as 'secret' does not contain any information on cover data collection measures applied.

21 Article 7, paragraph 1, point 8 of the Law on Parliamentary Oversight

c) Control hearing

Control and consultative hearings are among the mechanisms used to oversee the application of SSM. Until now, the Committee experienced *one case* of possible abuse of the SSM in relation to which it discussed the initiative on decision for a control hearing.

At the 21st session of the Committee for Security and Defense, held on 30 July 2010, the Initiative on decision for a control hearing of the NSA director and the Police director, submitted by five Committee members, was discussed '*with a view to gathering information and expert opinions on the implementation of policies and law in relation to statements and acts of the security structures aimed against the opposition politicians, NGO representatives and journalists, regarding the publication of Safet Kalic's wedding video on the internet*.'[22]

After discussing the initiative, the Committee adopted the *Conclusion* which demanded that the NSA director, in line with Article 68 of the Parliament's Rulebook, *deliver the information* on the issues raised in the Committee members' initiative, with a deadline set for the end of September 2010.[23] On 6 October 2010, the NSA notified the Committee members in writing that its officials were not tracking opposition, NGO and media representatives. The document bears the label 'secret'. MP from the Movement for Changes (PzP), Nebojsa Medojevic, underlined that it was an unnecessarily confidential document which only contains a polemic on MANS' accusations and a denial of tracking of this NGO's activists.

Control hearing did not take place. This is an example of inefficient work of the Committee which additionally points to the need to develop new, deeper mechanisms of parliamentary oversight of the use of SSM, as well as to the need to establish a link between the NSA internal control and the Committee, since there are only minimal chances that a potential organization of a control hearing would produce any new findings in this case.

22 The initiative took place after the leaders of the Network for the affirmation of NGO sector (MANS) requested information from the NSA on whether that institution was gathering and maintaining their personal data and received an answer stating that 'it has been concluded that responding to this request could prevent, i.e., jeopardize the execution of certain tasks undertaken by the NSA, so the Agency is not obliged to act in line with the legal provisions.' Such an answer was interpreted by the MANS employees as intimidation and pressure-exertion used to stop them from speaking publicly about corruption and organized crime.

23 'Performance report of the Committee of the 24th convocation of the Parliament of Montenegro', Podgorica, 3 September 2010.

Free access to information

From 2005 to 2009, the public was able to get access to information on the *number* of surveillance cases applied over mail deliveries and other means of communication. However, since the adoption of the Information Secrecy Act, the NSA has been precluding access even to that piece of information, declaring it secret.[24] Allegedly, 'such data are security-related and of special importance, whose publication and abuse would hinder, jeopardize or endanger the execution of NSA tasks.'[25] In contrast, precise data on approved and extended measures, as well as the legal basis for their approval, are publicly available, e.g., in the United Kingdom and France.[26] These statistics embody an important element of informing the public about the extent to which surveillance measures are applied over electronic communication. As such, they may help in generating a constructive dialogue with regard to this issue. It is also one of the criteria for assessing the level of democracy in a society. Based on the 2006 data, among the European countries, Italy applied this measure most frequently with the surveillance ratio of 76 persons per 100.000 citizens. Second place was taken by the Netherlands which kept under surveillance 62 persons per 100.000 citizens, and third by Switzerland with the ratio of 32/100.000.[27]

Recommendations:

- **By amending the Law on NSA:**

  -formulate the provision related to surveillance over electronic communication and mail deliveries more precisely, thereby explaining in detail what surveillance over electronic communication entails;

  - adopt a separate provision related to access to phone call lists, which would include time limits for the application of that measure;

  - complement the proposal for the application of measure with the reasons explaining why the application of other measures was inappropriate to gather the data in question, including a statement claiming that the application of measures is likely to produce expected results;

  - prescribe the obligation for NSA to deliver gathered material to the President of the Supreme Court / Panel of Judges, following the application of measures, for an '*assessment of the legality of application*' - during this assessment procedure, immediately after the judge's reading, part of the material non-related to the reasons which triggered the use of such measures should be destroyed immediately, as well as other personal data which are irrelevant for security, while the rest of the material could then be kept in the records;

  -prescribe that in the case of SSM application, upon the conclusion of the case, the individual who has been the subject of surveillance shall be informed, without his/her written request, and shall be granted insight into the gathered material, except in cases where national security is threatened;

- **Adopt a bylaw which would regulate the procedure of visit to the NSA in more detail, in order to allow for a more frequent use of this control mechanism, thereby providing more useful and meaningful information about the operationalisation and the application of SSM;**

- **Enable access to completed control reports of the NSA Internal Control;**

- **By amending the Law on Parliamentary Oversight of Security and Defense Sector:**

- adopt a provision which would oblige NSA to deliver a special report on SSM regularly, whose contents shall be prescribed in detail and which shall include:

---

24 The Supreme Court of Montenegro, in its verdict (Uvp. br. 174/10), confirmed the decision of the NSA of 15 February 2010, and the verdict of the Administration Court of 12 May 2010, in which NGO MANS is refused free access to information through delivery of a 'copy of the act containing data on number of persons whose mail deliveries and other means of communication were under the NSA surveillance in 2009.' It reads that: 'Pursuant to Article 16, paragraph 2 of the Law on NSA, registers and data records represent state, official or business secret. Those documents [...], in line with the Information Secrecy Act, are marked as "secret".'

25 NSA decision, No. 250-01-2699111, Podgorica, 20 May 2011 - upon request from the Institute Alternative for free access to information: number of requests for extension of measures, number of approved extensions of measures, number of measures approved individually on grounds of suspicion, number of suspensions of SSM application.

26 'Interception of communications in Albania: Legislation and Practice', Arjan Dyrmishi, IDM Center for Security Studies, June 2010, p.

27 'Italian bill to limit wiretaps draws fire', Duncan Kennedy, 11 June 2010

- number of cases when surveillance measures were ordered;
-number of persons whom surveillance measures were ordered for;
-number of persons who were data subjects of the surveillance measures;
-number of rejected requests for the application of surveillance measures;
-legal basis for ordering surveillance measures in individual cases;
-number and type of communication means kept under surveillance in individual cases;
-information on confirmed irregularities in the application of surveillance measures in individual cases;
-information on the number of data deliveries to other state bodies which resulted in a criminal procedure and a legally-binding verdict;
-information on the number of individuals notified to have been under SSM, including the number of those who were granted insight into the material gathered through SSM.

-adopt a provision which will oblige the Supreme Court to inform the Committee on the approved SSM, through a special report on SSM, whose mandatory content would include:

-number of written proposals of the NSA director addressed to the Supreme Court for its approval of SSM;
-number of approved/disapproved measures;
-number of requests for extension of measures;
-number of approved extensions of measures;
-number of measures approved based on individual grounds of suspicion;
-number of suspensions of SSM application;

-adopt a provision enabling the Supreme Court to inform the Committee for Security and Defense on individual cases in detail, upon request.

- **Establish the policy of free access to SSM-related information which do not pose a threat to national security, and enhance transparency of the NSA work.**
- **NSA should reconsider all decisions on document protection and consequently remove the label 'secret' from the unjustifiably protected documents and information.**
- **End the practice of storing documents and information, declared secret by a provision from the Law on NSA, if they are not an actual threat to national security, and allow access to them.**

Sources:

a) *Constitution of Montenegro*
b) *European convention on human rights and fundamental freedoms*
c) *Law on National Security Agency*
d) *Law on Parliamentary Oversight of Defense and Security Sector*
e) *Law on Personal Data Protection*
f) *Rulebook of the Parliament of Montenegro*
g) *Performance Report of the Committee for Security and Defense of the 24th Convocation of the Parliament of Montenegro*
h) *Regulation on more detailed conditions and manner of implementing measures of data protection*
i) *2006 Annual Performance Report of the National Security Agency*
j) *2007 Annual Performance Report of the National Security Agency*
k) *"Interception of communications in Albania, Legislation and Practice", Arjan Dyrmishi, IDM Center for Security Studies, June 2010*

Interviews:

b) *MP Predrag Bulatović, representative of the Socialist People's Party in the Committee for Security and Defense*
c) *MP, Borislav Banović, representative of Social-Democratic Party in the Committee for Security and Defense*
d) *Inspector general of the National Security Agency, Vlado Radović*
e) *Director of the National Security Agency, Vladan Joković, and his assistants Katarina Ćulafić and Goranka Serhatlić*
f) *President of the Supreme Court, Vesna Medenica*

Press articles:

c) *"Visit to the NSA: Opposition MPs control, but don't like to be controlled", Analitika - Information Portal, Section: Politics-News, 12 March 2010*
d) *"Italian bill to limit wiretaps draws fire", Duncan Kenneedy, 11 June 2010*

institut alternativa

About Institute Alternative

Institute Alternative acts as a think tank and a research centre, and its activities focus on the domains of good governance, transparency and accountability. Topics covered by the Institute's research activities, in which it exercises influence by providing its own recommendations are: parliamentary oversight of security and defense services, oversight role of the Parliament and its impact on the process of European integration, reform of public administration, public procurement, public-private partnerships, state audit and control of the budget of local authorities.

To date, Institute Alternative published the following reports / studies:

- Parliament of Montenegro and the process of European integration - Just watching or taking part?
- Parliamentary Inquiry in Montenegro - Oversight Tool Lacking Political Support
- Montenegro under the watchful eyes of Đukanović and EU
- Regulatory Impact Assessment (RIA) in Montenegro
- Control of the local self-governments' budget
- The State Audit Institution in Montenegro - strengthening its influence
- Report on democratic oversight of security services
- Think Tank - The role of Independent Research centers in Public Policy Development
- Public-Private Partnerships in Montenegro - Accountability, Transparency and Efficiency
- Public Procurement in Montenegro - Transparency and Liability
- The Assessment of Legal Framework and Practice in the Implementation of Certain Control Mechanisms of the Parliament of Montenegro: Consultative Hearing, Control Hearing and Parliamentary Inquiry
-Parliamentary oversight of the defence and security sector: What next?
-The Lipci Case: How not to repeat it
- The Case of the First Bank - Lessons for the supervisor and other decision makers
-Public Administration in Montenegro: Salary schemes, reward system and opportunities for professional advancement

Further information about Institute Alternative is available at:

www.institut-alternativa.org

CIP - Каталогизација у публикацији
Централна народна библиотека Црне Горе, Цетиње

ISBN 978-9940-533-18-2
COBISS.CG-ID 20423696