COMMUNICATIONS INTERCEPTION OVERSIGHT IN MACEDONIA

"Making The Impossible Possible"

Andreja Bogdanovski
Magdalena Lembovska

analytica
thinking laboratory...

Skopje, 2015

COMMUNICATIONS
INTERCEPTION OVERSIGHT
IN MACEDONIA

"Making The Impossible Possible"

Andreja Bogdanovski
Magdalena Lembovska

Design by Muhsin Güler

This report was developed within the "Framework Project - Fostering Parliamentary Oversight of the Security Sector in the Western Balkans," implemented by the Geneva Centre for Democratic Control of Armed Forces, DCAF (www.dcaf.ch) with funding from the Norwegian Ministry of Foreign Affairs. The authors of the paper are Research Fellows at Analytica think tank (www.analyticamk.org), an Associated Implementation Partner organization for the project in the Republic of Macedonia.

Contents

1.INTRODUCTION

Interception of communications represents one of the most efficient tools that authorities have in combating crime as well as acts that can endanger national security. Communications technology today is widespread and plays an integral part in our everyday lives through the use of our smartphones, e-mail accounts, online banking and even social networks like Facebook or Twitter. While technology rapidly develops and we are connected more than ever, crime related activities also morph, employing different tactics and methods while relying more and more on using communications technology. We have come to a point where countering 21st century crime undoubtedly requires 21st century methods which very often means more invasive access to our personal space constraining our privacy.

Having in mind that the interception of communications is one of the most intrusive measures which the state can employ in order to ensure the security of the country, exceptionally good oversight should be put in place. State security institutions such as the Counterintelligence Unit would normally resort to this technique when the other methods for data collection are not possible. While Macedonia has a post-communist legacy that in many aspects is perturbing efficient oversight performance, today's major oversight challenges relate primarily to problems that have occurred after Macedonia's independence in 1991. These include politicization of the security sector, lack of expertise, lack of political will, lack of oversight and accountability culture, etc.

This policy study re-surfaces the question of communications interception in Macedonia through looking into the most pressing issues affecting how this special investigative measure is implemented and focusing primarily on its oversight. It starts by providing an insight into the legal acts outlining the grounds for employing this measure and illuminating some of the inconsistencies. The study also takes a closer look into the state institu-

tions entitled to intercept communications such as the Ministry of Interior and Ministry of Defence, but also gives an overview into the Finance Police and the Customs, which as of 2012 received authorizations to intercept communications with the amendments of the Law on Communications Interceptions. The central component of this paper is the analysis of the state of oversight over the use of communications interception measures. For this purpose the policy study discusses the challenges that are primarily affecting the work of the Parliament in this segment but also it pioneers the idea for greater involvement of the Ombudsman in communications interception oversight in Macedonia.

For the purpose of this research the authors of the paper in December 2014 performed a field visit including a number of interviews with officials in Estonia's capital Tallinn in order to gain better understanding of the country's experience in performing oversight over communications interceptions. Estonia, similarly to Macedonia has a communist past and legacies from the previous system. Even though it has re-gained its independence in the beginning of the 1990's, the political establishment managed to build up professional, efficient and accountable public institutions, something Macedonia is still in the process of acquiring and in fact a main challenge which perturbs effective oversight.

CASE "PUC"

The urgency and necessity for writing a comprehensive and in-depth policy study on this subject cannot be better illustrated than by looking at the situation Macedonia is in since February 2015 with the presumed revelations of massive illegal wiretapping of allegedly more than 20.000 people. Macedonia's biggest opposition party SDSM[1] started revealing audio material of what appears to be telephone conversations between high government officials and journalists showing compelling evidence of corruptive behaviour, election fraud, media pressure and illustrating inter-par-

1 Social Democratic Union of Macedonia

ty political functioning of members of the ruling VMRO-DPMNE[2] party. With codename Puc, which is short for Coup-d'etat in Macedonian, the Ministry of Interior accused the biggest opposition party for illegally obtaining these materials. The main premise of the Government is that the opposition worked with foreign intelligence services aiming to destabilize Macedonia through the leaking of (according to them) manipulated materials. At the moment of writing of this policy study (April 2015), the Ministry of Interior has instructed the Public Prosecutor's Office to act on this case providing (according to them) evidence-based material confirming these allegations. Similarly, the opposition party has also filed criminal charges for illegal wiretapping, which make things more complex for the Public Prosecutor's Office, often time being subject to criticism about its lack of independence from the executive branch of power. As time passes by and more scandalous revelations see the light of the day, discussions on this topic are moving beyond the institutional framework and now have intertwined into a political battle between these two parties. International organizations such as the EU and OSCE are following the situation with great interest as well.

Analytica's researchers have an established track record of work related to intelligence governance and oversight. Over the years we have been strong advocates for enhancing the state of oversight of the intelligence services in order to prevent an outcome such as this one involving massive violations of the right to privacy. The research activities carried out for this policy study started in the summer 2014 and the overlap with the actual situation is a coincidence. Due to its comprehensiveness and strong focus on oversight we believe that through this policy study we contribute with concrete measures in order to prevent a misuse of the intelligence services on such a massive scale in the future.

2 Internal Macedonian Revolutionary Organization – Democratic Party for Macedonian National Unity

2. LEGAL FRAMEWORK

When it comes to communications interceptions, the Macedonian legal framework is treating this matter in several laws: Law on Communications Interception, Law on Electronic Communications and the Law on Criminal Procedure. Over the years there have been a few alterations of the legislation, providing greater authorizations while at the same time legally speaking enhancing the oversight possibilities, especially those of the Parliament. For example the parliamentary Committee for Supervision of the Application of Communication Interception Techniques by the Ministry of Interior and the Ministry of Defence was established in 2006 with the adoption of the Law on Communication Interceptions.

2.1. LAW ON COMMUNICATIONS INTERCEPTIONS

The primary function of the Law on Interception of Communications (adopted 2006, amended 2008 and 2012) is to legislate the procedure for interception of communication in Macedonia, processing, storing and using the data as well as provide information on the oversight.[3] With the changes of the Law on Criminal Procedure, back in 2010, there were also changes in the procedure for authorizing communications interception. The Public Prosecutor's office received increased competences in this segment where it can initiate request for authorizing this measure to the responsible judge. According to the law, the Court can authorize interception of communications relevant to the security and defense of the country in the following cases: preparations of criminal acts against the state, criminal acts against the armed forces and against international law and humanity. Additional categories involve encouragement, organization or participation in armed attack against the Republic of Macedonia, or incapacitating its security sector.[4] Having in mind the seriousness of the above-mentioned cases the Law authorizes the Minister of Interior and the Minister of Defence to be able

3 Law on Interception of Communications (as last amended in 2012) Article 1
4 Ibid. Article 29

to send a request to the Public Prosecutor for employing such methods.[5] The Public Prosecutor continues the procedure by requesting approval from a High Court Judge.

Some of the major updates of the amendments of the Law on Communication Interception included extending the range of activities that now fall under "communications" such as software based platforms like Skype, Viber, WhatsApp etc. Considerable criticism can be seen when discussing the possibility to intercept communication by verbal order issued by a judge. Before changing the law, there was a legal provision enabling state institutions to intercept someone's communications if there was a matter of urgency and there was a clear need for communications to be intercepted. According to the Law on Communications Interceptions, the benchmark set for verbal permission referred to cases which have risk for death of one or more persons, heavy bodily injuries of one or more persons, material damage of large scale property or indications for escape of criminals who committed a crime that entails sentence of life in prison.[6] However, the new provisions brought by the changes of the law in 2012 determine that interception of communications upon verbal order could take place in urgent cases, when there is danger of causing irreparable damage to the criminal procedure.[7] This sounds very vague and provides broader framework for the authorities to intercept communications without having written order from the court.

The maximum length for intercepting communications was extended from the original 30 days to four months for criminal cases with possibility for extensions up to 14 months in total (previous provisions limited maximum extension up to 12 months). Maximum length of application of interception of communications in cases of threats towards the security and defence of the country is 6 months with possibility of extensions up to 2 years in total. Another major novelty which the amendments of this law brought is the expansion of state institutions that may now intercept

5 Ibid. Article 30

6 Law on Interception of Communications (as amended in 2008) Article 14

7 Law on Interception of Communications (as last amended in 2012) Article 11-a

communications. These now include: Financial Police, the Public Prosecutor and the Customs Office.

2.2. LAW ON ELECTRONIC COMMUNICATIONS

This law was firstly introduced in 2005 and underwent several changes up to 2014 when a new law on electronic communications was adopted.[8] It can be considered to normatively regulate the relationship between the authorities allowed to intercept communications (Ministry of Internal Affairs – counterintelligence service, Ministry of Defence etc.) and the telephone operators. The focus of the research which is interception of communications is regulated in Articles 175 and 176 of the Law on Electronic Communications, providing a rather technical view on the interception of communications architecture. Consequently, the law obliges all operators to install technology that would enable transfer of users' data to the authorities entitled to intercept communications. The Law however is not clear whether such a technology like for example optical cables should be installed to all five (at the moment) institutions authorized to intercept communications or to only one. The phone companies, according to Article 175, are tasked to provide real-time interceptions of communications.[9]

Another segment of the Law of Electronic Communications represents the obligation (Article 176) under which phone companies should store data from the electronic communications (data retention), which do not necessarily come as a result of an interception order but from the day-to-day functioning of the users' phones such as call listings, location, etc. The aim of such intrusive measures is to allow access to these data for the purpose of stopping or revealing criminal acts, conducting a criminal proceeding or when it is required for the security and defence of the country.

When the Law was enacted, telecommunications operators had remarks on the text of the law, primarily relating to the increase of costs incurred

8 Official gazette of the Republic of Macedonia no. 39/2014
9 Law on Electronic Communications, Article 175

from the adoption of the law, such as article 175 (sect. 3) where operators before purchasing communication interception hardware and software must do so by specifications given by relevant state authorities who can intercept communications.[10]

Another segment which deserves attention is the length that personal communication data can be stored and kept by the telecommunication operators. This data includes a range of activities and (personal) information starting from the identity of the caller, callers registry list, name and address of the number holder, pin code/password when using SIM card/ internet connection, IP address, time and date of the calls, current GPRS location, etc. According to this Law on Electronic Communications operators should keep this data for a period of 12 months.

2.3. LAW ON CRIMINAL PROCEDURE

The Law on Criminal Procedure determines the procedure for application of all special investigative measures, including interception of communications. Also, it regulates the conditions that have to occur so the competent authorities could request and order such measures.

Interception of communications was part of the package of special investigative measures that were introduced for the first time in Macedonia when the Law on Criminal Procedure from 1997 was amended in December 2004. In 2010, the Parliament adopted a new Law on Criminal Procedure and its implementation started in December 2013. According to the existing legislation, basis for ordering special investigative measures could be grounds for suspicion about:

1. Criminal acts for which foreseen is a prison sentence of at least four years and are being prepared, are being perpetrated or have

10 T-Mobile Macedonia suggestions to the draft law on electronic communications. https://ener.gov.mk/default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=kD/JU8uL687IkYMWVEaxNw p. 10, last accessed 10.02.2015

been perpetrated by an organized group, gang or other criminal enterprise;

2. Criminal acts that are specifically listed in the Law on Criminal Procedure, including: murder, kidnapping, illicit trafficking, smuggling, money laundering, criminal enterprise, terrorism etc.;

3. Criminal acts against the country (Chapter XXVIII), criminal acts against humanity and international law (Chapter XXXIV) from the Criminal Code.[11]

Back in 2004, the law envisaged "wiretapping and recording in one's home or other premises and entering those premises for purposes of creating conditions to monitor communications" as a unique special investigative measure. As the nature and the type of communication techniques evolved, in 2010 the legislators decided to create three separate measures: 1) Intercepting and recording of telephone and other electronic communications, 2) monitoring and recording in homes and other premises and entering those premises for purposes of creating conditions for interception of communications, 3) insight in realized telephone and other electronic communications. The implementation of the new law, including usage of these special investigative measures as defined, started in December 2013.

Concerning the procedure, there are substantial changes brought by the new Law on Criminal Procedure. The Public Prosecutor now receives major role in the procedure and leads the investigation i.e. collection of evidence. This means that when requesting application of interception of communications, the Public Prosecutor is the first filter that needs to ensure lawful interceptions. Then, upon an elaborated written request to the competent judge, the court might provide approval. In practice, this should ensure two-level control of the measure – one from the public prosecution and one from the courts. It is also important to mention that in case the public prosecutor decides to waive criminal prosecution, or the collected data do not have value for the procedure, those data obtained using special

11 Law on Criminal Procedure from 2010, Article 253

investigative measures should be destroyed.[12]

In terms of transparency, the Law on Criminal Procedure includes important provision on reporting to the Parliament. The Public Prosecutor has an obligation to submit an annual report to the Parliament including comprehensive statistical data on application of special investigative measures, and also information on results and costs of implementation.[13] These reports have special value for the parliamentary committees that could collect, match and discus data obtained from different institutions. Even in cases when some of the institutions fail to submit reports, the Public Prosecutor reports could be valuable resource and indicator of performance.

2.4. HARMONIZATION WITH EUROPEAN STANDARDS

Macedonia's legislation in many respects is closely following the one of the EU including data protection and data privacy. This is mainly a result of country's desire to join the EU where alignment with legislation is one of the criteria for becoming fully-fledged member.[14] Macedonia is also a signatory of the European Convention of Human Rights (ECHR) which is also putting a great emphasis on the protection of privacy. Article 8 of the ECHR refers to the Right to respect for private and family life clearly demonstrating the importance of protection of correspondence. Any sort of interference from the public authorities in this right should be clearly in "…accordance with the law and is necessary in a democratic society in the interests of national security, public safety…for the prevention of disorder or crime..."[15] All of the signatories are obliged to comply with the Conven-

12 Ibid. Article 261

13 Ibid. Article 271

14 The 2014 European Commission Progress Report describes Macedonia to have advanced level of legislative alignment, at strategic and institutional level across all areas of the EU acquis.

15 European Convention of Human Rights http://www.echr.coe.int/Documents/Convention_ENG.pdfp 11.

tion in order to safeguard highest democratic principles.

The EU on the other hand deals with the issue of data privacy and data protection on a more operational level establishing rules of conduct for a Union of 28 member states. More striking legal acts in this area can be seen in the following EU Directives: 2002/58/EC, 2006/24/EC and the 2014 European Court of Justice ruling on data retention. EC Directives provide reassurance that EU member states will act in a way that do not violate confidentiality of communications. For example Article 5 of the Directive 2002/58/EC states that "…[member states] shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data…without the consent of the users concerned, except when legally authorized to do so…"[16] Moreover, Article 15 of the same Directive mentions exceptions when public authorities can access data including questions related to national security. At the same time this directive introduces the possibility for EU wide data retention which is elaborated in details in 2006/24/EC also known as Data retention Directive.

Many similarities of the Data retention Directive can be found with Macedonia's Law on Electronic Communications especially in the segment of types of data authorities can access such as location of user, calling telephone number, time and date of logging in and logging out of the internet service etc. The Directive however is rather flexible in terms of the time period for which EU member states/telecommunications operators can retain data. The minimum it prescribes is 6 months and maximum of 2 years. Most of the retained data in EU however is between 1-6 months old.[17] For a comparison Macedonia's legislation limits the retention of data to 12 months. In terms of reporting of the statistics on the retention of data,

16 Directive 2002/58/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

17 European Commission, DG Home Affairs, Statistics on request for data under the Data Retention Directive, October 2013, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf

Macedonian Criminal Procedure Act stipulates that the Public Prosecutor delivers a publicly available report to the Parliament including statistics on the use of Special Investigative Measures, including retention of data. However such a report has not been submitted for 2013 and 2014. Separate statistics from before are not available because prior to 2013 retention of data was not a separate special investigative measure and the Public Prosecutors Office does not provide a breakdown.

A U turn for EU's Data retention Directive was the 2014 judgment by the European Court of Justice originally initiated by the High Court in Ireland and Austria's Constitutional Court. ECJ's ruling annulled the Directive on the basis of infringement of civil liberties due to providing national authorities access to personal information at large scale. More precisely Court's decision was centered on the right to respect for private life and the right to the protection of personal data.[18] The Court has acknowledged the public interest when it comes to maintaining national security, fight against organized crime but found that the Directive failed to satisfy the criteria on proportionality.[19] The almost one year old ruling by the ECJ has created mixed reactions among EU member states but there seems to be a consensus of the need for review of national legislation which would respect the ruling, until EC comes up with proposal for new directive in this area.[20] Many EU member states like the UK, Netherlands and Luxembourg have decided to continue with their data retention policies stemming from the fact that such activity (according to them) is a paramount for successful criminal investigations and national security issues.[21] Even though the data retention directive is not in force anymore member states still have the

18 Court of Justice of the European Union, Press Release No.54/14, The Court of Justice declares the Data Retention Directive invalid, 08.04.2014, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
19 Ibid.
20 Claire Francois, ECJ's invalidation of EU Data Retention Directive creates confusion over telecommunications service providers' data retention obligations, Privacy Law Watch, 2014, available at: http://www.hunton.com/files/Publication/dec9c9bc-0527-4620-9664-ab40152923be/Presentation/PublicationAttachment/39d39846-4efd-473d-81da-ea264bfbb90d/ECJs_Invalidation_of_EU_Data_Retention_Directive.pdf
21 Ibid.

right for this practice based on Directive 2002/58/EC which mentions this possibility without going into further explanation.[22]

Apart from looking into the use of special investigative measures including data retention from the civil liberties perspective, equally important issue is their invaluable use when it comes to criminal investigations as well as national security matters. Due to the highly gated Macedonian security sector, information about concrete examples where the use of special investigative measures proving helpful in investigation or prevention of a threat is not available. In order to illustrate their usefulness on EU soil, the European Commission in 2013 published a report providing evidence of real life cases where data retention have been found crucial in investigating criminal offences such as: terrorism, child pornography, murder, manslaughter etc. On terrorism related offences the report states that "investigations often require time in order to establish a clear pattern and relationships between multiple events and so to expose not just individual suspects but whole criminal networks…"[23] The following cases in Germany explain this with concrete examples.

22 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

23 European Commission, DG Home, Evidence for necessity of data retention in the EU, March 2013 pg. 4, available at: http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf

TERRORISM RELATED CASES

Germany[24]

1. Individuals were suspected of supporting Al-Qaida and the Uzbekistan Islamist Movement by distributing propaganda material on the Internet and trying to attract supporters for their cause. The Internet access provider had not retained the IP address of one user who had logged in to establish an Internet video channel for those purposes, and investigators were unable to pursue that part of the inquiry.

2. In an Internet forum on 12 April 2010 a video of a terrorist organisation was made available through various Internet links. One of these links had been created by an unknown person registered under a certain e-mail address. An inquiry concerning the e-mail address with the responsible e-mail service provider revealed that it had been registered only a day before the release of the video. The IP address had been allocated by a major ISP, but as seven days had already elapsed the ISP said they it did not hold the IP address details. The person could not be identified and the case remains open.

3. AUTHORIZED INSTITUTIONS

3.1. MINISTRY OF INTERIOR

The Ministry of Interior is the most important actor when it comes to interception of communications. Both organizational units – the Directorate for Security and Counterintelligence and the Bureau for Public Security have authorization to implement such activities.

The Directorate for Security and Counterintelligence performs activities related to protection from terrorism, severe forms of organized crime and other activities aimed at threatening or violent destruction of the dem-

24 Ibid. pg 7

ocratic institutions established by the Constitution[25] and therefore application of interception of communications is one of the essential methods of data collection. On the other hand, the Bureau for Public Security has access to this special investigative measure for the purpose of criminal procedures related to criminal offences specifically listed in the Law on Criminal Procedure. According to Gordan Kalajdziev, Professor at the Law Faculty in Skopje, while the interception of communications as a data collection method in the criminal procedure is strictly regulated with the adequate Law on Criminal Procedure, the authorizations of the Directorate for Security and Counterintelligence are not regulated with this primary regulation, leaving space for additional legal arrangements.[26]

Statistical data concerning the usage of the measure are classified as "strictly confidential" and "top secret" within the Ministry of Interior.[27] The European Commission progress report on Macedonia in 2011 pointed out that the number of interceptions used in organized crime cases is relatively low and criticized the direct role of the Minister in the procedure.[28] Afterwards, the Law on Communication Interceptions was amended, providing a better enabling environment for the Ministry. While the Ministry of Interior denies access to any information on applied interceptions, this is not the case with the courts and public prosecution. From available public data it could be concluded that the usage of the special investigative measure interception of communications increased after the changes in the legislation in 2012.[29] A vaguely regulated area and lack of transparency on the issue once again highlight the need for an appropriate controlling mechanism.

25 Law on Internal Affairs, Article 23

26 Gordan Kalajdziev, Professor at the Faculty of Law Skopje (personal interview in Skopje, 24 December 2014.)

27 Information gained using the Law on free access to information from public character

28 European Commission Progress Report on Macedonia for 2011

29 Concrete data could be found in Section 4: Interception of communications through numbers.

3.2. MINISTRY OF DEFENCE

The Ministry of Defence has a special unit tasked for defence intelligence and counterintelligence. It is authorized to intercept communications only within specified frequencies (high, very high and ultra high frequencies) specific to defence needs. The Law on Interception of Communications regulates that the Ministry of Defence is entitled to apply this measure when it is needed for the protection of state security and defence and such request can be submitted by the Minister of Defence or a person designated by the Minister. The Law on Defence does not specify this area any further. It only says that the Ministry of Defence performs intelligence and counterintelligence for the defence needs as well as detection and prevention of specific crimes.[30]

Intercepting communications for defence purposes is a highly classified area so there is very little information available on the topic. The Ministry of Defence claims that they have not intercepted communications in the last few years.[31]

3.3. CUSTOMS ADMINISTRATION

Established in 1992, the Customs Administration is a state administration authority within the Ministry of Finance with the status of a legal entity. Besides performing what is meant by customs matters (customs supervision and control, customs clearance of goods, collection of fees etc.), this state administration authority has the fiscal interests of the state in focus as well as suppression of illicit trade, protection of people and environment and criminal intelligence.[32] The Customs Administration is one of the institutions that gained interception of communication powers as a special investigative measure with the recent changes of the law in 2012.

30 Law on Defence, Article 20
31 Information gained using the Law on Free Access to Information from Public Character. Requested data refer to period 2010 - 2014
32 Law on Customs Administration

Concretely, the Customs Administration can apply such measures in criminal investigations concerning criminal offenses punishable by a sentence of imprisonment of at least four years, criminal offenses committed by an organized criminal group, or criminal offenses listed in the Law on Criminal Procedure, mainly related to illicit import, export and transit of goods, money laundering, illegal possession of weapons, human trafficking etc.[33] The request for approval of application of the measure is submitted by the representative of the Customs Administration who runs the case.

Since the Customs Administration has received such an authorization, it is unclear whether it has utilized it. In the time when these changes were adopted, the Customs Administration did not have capacities for applying the measure nor did the law envisage financial implications for acquiring the necessary equipment and human resources.[34] When asked about the number of submitted requests for application of intercepting communications, the Customs Administration refused to answer, explaining that such information would cause significant damage to investigative and criminal proceedings.[35]

On the question referring to existing human and technical resources, it answered that the Customs Administration possesses human resources not only for application of this concrete measure, but also for all other special investigative measures. However, the information about the technical capacities is not available for the public on the basis that by doing so "it will reveal information about a document which is in a preparation stage" and "the information will not be correctly understood."[36] The European Commission Progress Report on Macedonia for 2014 highlights that the Customs Administration should "acquire technical capacity to independently carry out special investigative measures, which fall within its legal mandate".[37]

33 Law on Criminal Procedure, articles 47 and 253
34 Proposal for Law amending the Law on Interception of Communications
35 Information gained using the Law on Free Access to Information from Public Character
36 Ibid.
37 EU Commission Progress Report on Macedonia 2014, pg. 44

The strategic documents of the Customs Administration[38] vaguely say that one of the priorities of this state administration authority is improvement of the customs intelligence system and capacities, but there is no other concrete information about further steps or timeline. Publically available evidence for criminal charges brought by the Customs Administration in 2014 does not imply application of such measure – most of them are result of customs supervision and control when entering the country or suspicious invoices.[39]

3.4. FINANCIAL POLICE

The Financial Police was firstly established in 2003 as a state administration authority within the Ministry of Finance. Its primary role, then, was to perform investigations upon request by the Public Prosecutor, Ministry of Finance, Ministry of Internal Affairs, Customs Administration, Administration for Prevention of Money Laundering or ex officio.[40] With the new Law on the Financial Police[41] from 2007, it obtained the status of legal entity as Financial Police Administration with authorizations for pretrial proceedings and investigations. Currently, the Financial Police operates under the most recent Law on the Financial Police from 2014.[42]

Its powers for applying interception of communications as a special investigative measure were acquired along with the Customs Administration in 2012. However, the Financial Police has more restricted authorizations, meaning that it could apply the measure only in cases related to detection and investigation regarding crimes involving illegal property of significant value, such as money laundering, illicit trade, smuggling, tax evasion etc. As

38 Strategic plan 2013 – 2015 and Strategic plan 2014 – 2016, both available at: http://www.customs.gov.mk/DesktopDefault.aspx?tabindex=0&tabid=58
39 available at: http://www.carina.mk/DesktopDefault.aspx?tabindex=0&tabid=243
40 Law on Financial Police, Official Gazette of the Republic of Macedonia no. 55/02
41 Law on Financial Police, Official Gazette of the Republic of Macedonia no. 55/07
42 Official Gazette of the Republic of Macedonia no. 12/14

was the case with other authorized institutions, request for application of the special investigative measure communications interceptions is decentralized and submitted by the officer leading the case.

The Financial Police did not answer Analytica's questions submitted using the Law on Free Access to Information from public character.[43] Also, there is no publically available information if the Financial Police has equipped itself with the proper human and technical resources and whether it has any successful operations in the field. According to the European Commission Progress Report for 2014, the Financial Police (along with the Customs Administration) still has inadequate human and technical resources which lead to limited application of special investigative measures.[44]

4. INTERCEPTION OF COMMUNICATION THROUGH NUMBERS

Table 1 shows statistical data obtained from the Primary Court Skopje 1 using the Law on Free Access to Information regarding received requests from all authorized institutions and issued orders for application of the special investigative measure interception of communications. As it can be seen, in 2012 the numbers are doubled compared to the previous year and keep the same pace in the year that followed. 2012 was the year when the Law on Interception of Communications was changed enabling decentralization of the usage of measure and removing the direct role of the Minister in submitting requests. However, what is worrying is the fact that the number of requested orders for application of the measure equals the number of issued orders – there is no single case throughout the years when the Primary Court Skopje I said "no" to the authorities. This could imply several conclusions. On the one hand, it questions the ability and expertise of the judges to assess the necessity and proportionality of the measure, especially taking into consideration the "ultima ratio" principle, which means that such measure shall be applied only if the data cannot be

43 According to the Financial Police Administration, requested information is not information of public character

44 European Commission Progress report for Macedonia for 2014 pg. 51

collected via less intrusive measures. On the other hand, all of the persons interviewed in Macedonia for the purpose of this paper[45] expressed their concerns that the Ministry of Interior maintains a superior role over the judiciary and there is pressure on the judges to approve everything that is requested.

Primary Court Skopje I	Received requests	Issued orders
2010	103	103
2011	102	102
2012	216	216
2013	226	226
2014 (up to May 2014)	77	77

Table 1: *Number of received requests and issued orders for interception of communications by the Primary Court Skopje I*

When asked about the concrete criminal deeds for which application of the measure have been ordered, the court provided a list of criminal offenses as defined in the Criminal Code, including: murder, kidnapping, production and narcotic drug trafficking, unlawful manufacture, possession, and sale of weapon and explosives, bribing, trafficking in human beings, smuggling etc., but there have been also case(s) of international terrorism. However, there have been also cases such as "forging documents" (article 378), "using a document with false content" (article 380) or "forging official document"(article 361) for which the Criminal Procedure Act does not envisage usage of special investigative measures, unless there is an organized criminal group involved.

45 Full list of interviewees available in the Bibliography section.

Special investigative measure	Requests submitted to investigative judge		
	Year 2010	Year 2011	Year 2012
Monitoring of communication and entrance in home or other premises for creating conditions for monitoring of communication	14	28	33
An insight and searching in the computer system, confiscation of computer system or part of it or the data -base for storing of the computer's data	5	1	5
Secret surveillance, monitoring and visual-sound recording of persons and objects with technical equipment.	27	19	31
Simulating purchase of objects, as well as simulating bribery and simulating acceptance of the bribe	19	13	11
Controlled delivery and transport of persons and objects	4	1	2
Using people with hidden identity for monitoring and collecting information or data	14	9	8
Registration of apparent (simulated) companies or usage of the existing companies for collecting data	1	0	0

Table 2 *Number of requests for application of special investigative measures to investigative judge submitted by the Public Prosecution*[46]

Table 2 shows statistical data obtained from the annual reports of the Public Prosecution submitted to the Parliament. However, one must be

46 Source: Annual report for the work of the Public Prosecution in Macedonia for 2010, 2011 and 2012

careful when comparing these data because they refer to a number of cases and not number of persons against whom the measure have been applied. There could be orders for several persons in regard to one criminal case. What could be easily concluded is that secret surveillance measures and interception of communications are the most frequently ordered from the whole arsenal of special investigative measures.

From the annual reports of the Public Prosecutor it is evident that there are new suspects of terrorism every year.[47] This could be one of the topics of discussion for the parliamentary committees. In order for the Committees to discuss oversight matters in greater substance MPs need to follow and be well informed on the general security situation in Macedonia. Issues such as terrorism as well as other forms of serious organized crime are areas where use of special investigating measures including communications interceptions are playing important role when conducting investigations. This way MPs can get a better idea about the threats the country has been facing and initially help in questioning whether use of special investigative measures were proportionate to the threats. The annual reports of the Public Prosecutor are helpful in this direction because they show the intensity of using these measures. For example MPs can do a comparative analysis over the years of the use of wiretapping and in theory spot drastic increase/decrease of their use by state authorities. This can then be a good foundation for asking questions to the representatives from the Counterintelligence Service on this matter.

5. STATE OF OVERSIGHT

When it comes to the oversight of communications interception in Macedonia, legally speaking even though some obstacles remain, these in theory should not impede effective oversight. Macedonia has gone one step forward in the legal and to somewhat institutional sense compared to other European countries when for example looking at the specially

47 Ibid.

designated Parliamentary Committee tasked to oversee the interception of communications as a separate special investigative measure. However in practice the work of this committee has not lived up to the expectations. Ever since its establishment in 2006 it has shown negligible track record of providing effective oversight.

The Parliament is not the only place where control and oversight should be exercised. Internal control exercised within the institutions performing interception of communication and those authorising it should also be present and provide an additional layer of oversight. Additionally, independent state institutions such as the Ombudsman, State Audit Office or the Directorate for Personal Data Protection can act as powerful correctors of any wrongdoings the authorities entitled to intercept communications can be doing, hence providing holistic oversight. Speaking in cumulative sense, these institutions also fail (to a different extent) in providing effective oversight.

This section however only focuses on the Parliament and the Ombudsman when talking about oversight of the measure interception of communications, mainly because of their wide ranging competences in this segment such as the possibility for field visits, access to classified information, initiating and adopting legislation and their respective role in protection of human rights.

5.1. MACEDONIAN PARLIAMENT

The oversight exercised by the Macedonian Parliament when it comes to interception of communications is exercised primarily through the work of the competent parliamentary committees, but there are also mechanisms that could be used on plenary level such as parliamentary questions.

When it comes to overseeing interception of communications, Macedonian Parliament has gone a step ahead, creating special committee just for this purpose. The **Parliamentary Committee for the Supervision of the Application of Communication Interception Techniques by**

the Ministry of Interior and the Ministry of Defence (herein Committee supervising communications interception) was introduced with the adoption of the Law on Communications Interceptions in 2006. When the Financial Police and the Customs Administration acquired powers for application of special investigative measures in 2012, consequently the Committee became also their oversight body in this regard. The oversight is performed from the aspect of legality in the application of the measure.[48] Decisions are made with majority votes[49] and it has powers to request necessary information from the state institutions and form working groups.[50]

Another relevant Committee is the **Committee supervising the work of the Directorate for Security and Counterintelligence and the Intelligence Agency** (herein Committee supervising intelligence services). This Committee provides general oversight of the services, especially in regards to respecting the law in the work of the intelligence and counterintelligence service and respecting the freedoms and rights of the citizens, companies and other entities. Moreover, the Committee is entitled to consider issues regarding the methods and means used by the services as well as their financial, personnel and technical facilities. In practice, their work mainly consists of discussing annual reports and annual programs of the intelligence services. Those reports would not be complete unless they contain information on the data collection methods such as interception of communications. However, throughout the years, there have been challenges such as: receiving the reports from the services with delays, receiving incomplete information, lack of communication with other stakeholders etc.[51]

The **Committee on Defence and Security** is the third committee working on security related issues. Although one of the competences es-

48 Website of the Macedonian Parliament
49 Law on Interception of Communications, Article 36-a
50 Rules of Procedure of the Committee
51 The work of this Committee up to 2012 is analyzed in:
Andreja Bogdanovski and Magdalena Lembovska Towards 2nd generation of SSR in Macedonia, Analytica think tank, available at:
http://analyticamk.org/images/stories/books/pub-ssr-web.pdf

tablished by Decision of the Parliament is performing oversight in the security and defence domain, the work of the Committee comes down to discussing draft legislation.[52] Moreover, some of the members of this Committee do not have security clearance which limits their access to classified information.[53]

Another Committee that could play certain role is the **Standing Inquiry Committee for Protection of Civil Freedoms and Rights.** Among other competences, it is supposed to review complaints from the citizens and to take position upon them. This gives it an opportunity to consider concrete cases where citizens believe their right to be infringed. An important feature of this parliamentary body is that its findings represent basis for starting procedure for accountability of public-office holders. However, this Committee is not visible nor recognized for the public, especially taking into consideration that the Committee meets max 1-2 times per year (there were no meetings throughout year 2014).

Finally, the **Committee on Finance and Budget** discusses financial consideration. This provides different layers of oversight at different stages. For example this committee is supposed to be active when there is an adoption of a new budget or a rebalance of an existing one. It would be expected that a debate among MPs occur if for example the proposed budget entails (sudden) increase of money allocated for purchasing equipment for the needs of the Counterintelligence Service.[54]

Apart from the Committee discussions, there are other oversight mechanisms. Parliament's plenary sessions, including Parliament's **Q&A ses-**

52 Source: minutes of the sessions of the Committee on Defence and Security published on Parliament's website

53 Oftentimes, the MPs that are part of the special committees for intelligence oversight (and accordingly have security clearance) are also part of the Committee on Security and Defense

54 More on financial oversight of the intelligence services in Macedonia and the region could be found in:
Magdalena Lembovska, Comparative analysis of regional practices for parliamentary financial oversight of the intelligence services, Analytica think tank, available at: http://analyticamk.org/images/stories/files/report/Financial_oversight_english.pdf

sions are good opportunity for the MPs that are not part of the adequate parliamentary committees to pose questions to the ministers and other officials. Moreover, it is also an opportunity for the committee members to pose direct question instead of waiting for the committee to convene. However, the classification of the materials once again limits more substantial discussions.

Interpellation or a non-confidence vote could be raised for the work of individual members of the Government, the Government as a whole or any public official. So far, there have been 3 initiatives for interpellation of the most recent Minister of Interior (August 2006 – May 2015), whereas one of the initiatives was directly connected with usage of special investigative measures.[55] All of them were unsuccessful and this is the case with all such motions throughout the years. In spite of the fact that there has never been a case for a minister or public official to leave a function due to such motion, this is an important mechanism for the public to get acquainted with the work of particular office-holder and possible reasons for no confidence. The MPs discuss on the interpellation the whole day in presence of the summoned minister.

The Law on the Parliament envisages holding o**versight hearings** conducted by the committees in order to obtain information in relation to the establishment and the implementation of the policies, the implementation of the laws and the other activities of the Government and the state institutions. The invited representatives have an obligation to be present at the meeting on which an oversight hearing is held[56]. In 2012, the main opposition party SDSM announced a list of future oversight hearings where two out of seven were security related. The first one had to do with the budget and expenditures of the Directorate for Security and Counter – Intelligence and the other one was for the case "Campaign"[57] and the special

55 The discussion on the interpellation took place on 13th of February 2012 and among other things, had to do with the "Case Campaign" and limiting the competent Committee to perform oversight on the case.

56 Law on the Assembly of Republic of Macedonia, article 20

57 "Campaign" refers to the case of Mr.Ljube Boshkoski, leader of an opponent

investigative measures used by the MoI.[58] It was announced in July 2012, but after the summer holidays, the idea vanished.

Public debates on legislation are one more mechanism where the MPs could provide their input. An example of this is the public debate organized when the Law amending the Law on interception of communications was in the adoption phase in 2012. However, the public debate was not initiated by any of the committees working on security issues, but by the National Council for European Integration (another parliamentary body). Nonetheless, this public debate was a good example where all interested parties were invited and contributed with their views on the proposed law (including state institutions, CSOs, academia and other experts.). As a matter of fact, the Committee supervising interception of communications did discuss the proposal on its committee session and even invited CSOs representatives and other external experts to enrich the discussion.

5.2 IDENTIFIED CHALLENGES

Even though there are different levels of oversight present in the Parliament this model has not shown satisfactory results in practice. Over the years Macedonia has shown backslide in the quality of oversight exercised by the Parliament and especially in the segment of oversight of the intelligence services including also the interception of communications. Committees that meet maximum 2-3 times per year could not be considered to be watchdog of the intelligence services. Moreover, their agenda mostly consists of discussing their own rules of procedure or annual reports of

political party who was arrested and sentenced to 7 years in prison because of illegal funding of the party's campaign and abuse of office. His family and supporters are claiming that the case was mounted and set due to his fierce criticism towards the actual Government.

58 Опозицијата решена преку Собранието да ја контролира Владата [Opposition determined to control the Government through the Parliament], Kapital, 05.07.2012, available at: http://www.kapital.mk/MK/makedonija/86076/opozicijata_reshena_preku_sobranieto_da_ja_kontrolira_vladata.aspx

the services sent to them with delays.[59] While there has been at least track record of discussing EU progress reports[60] and the National program for adoption of the acquis communautaire[61] in the past, each of the two committees (Committee supervising intelligence services and the Committee supervising interception of communications) met only once in 2013. Due to the absence of the Opposition from the Parliament, the two committee overseeing intelligence could not even be formed in 2014 in full composition and start working.[62]

However, any kind of oversight, and especially the one over the measures that cause clear breach of human rights if misused, such as the interception of communications requires a reciprocal approach. On one hand it is the Parliament with all its capacity which should act as a watchdog while on the other, state institutions should also be responsive when it comes to their accountability to other state institutions, such as towards the Parliament. This is especially important in regards to the oversight and accountability culture among the intelligence services, which is clearly lacking. It is appropriate, for example, for the Director of the Counterintelligence Service to be present and personally answer questions to MPs about the annual reports of the activities of the Counterintelligence Service, something we have not witnessed since his appointment in 2006. The MPs have been also complaining on insufficient information provided by the intelligence services.[63]

59 More about the work of the Parliament could be found in:
Andreja Bogdanovski , "Case study: Macedonia" in *Almanac on Security Sector Oversight in Western Balkans,* Belgrade Center for Security Policy and Geneva Centre for Democratic Control of the Armed Forces

60 Committee for supervising the work of the Directorate for Security and Counterintelligence and the Intelligence Agency (2011-2014), committee meeting no.2, held on 17.10.2011

61 Committee for the supervision of the application of the communication interception techniques by the Ministry of Interior and the Ministry of Defense (2011-2014), Committee meeting no. 7 held on 27.02.2012

62 The Committee supervising intelligence services held one meeting chaired by a MP appointed by the Speaker on 09.12.2014. At the meeting, it established its Rules of Procedure

63 For instance, in a statement for newspaper Utrinski in 15.05.2012, Mr. Goran

The reasons for this might be traced by an absence of political will, lack of knowledge and expertise and party politics.

The Macedonian Centre for European Integration conducted a survey in 2014 on political culture, Europeanization and fears in Macedonia where a staggering 63,6% of the interviewed citizens believe that Macedonian intelligence services intercept the communications to those which are opponents to the current government.[1] 20,1 % were undecided and only 16,3% of the citizens believed that this was not true. After the revelation of illegally intercepted communications of politicians and other public persons in February-March 2015, there was another public opinion survey conducted by two other national CSOs[2] and TV Telma. The results showed that 43% of the citizens believe that their privacy has been infringed and the percentage is higher among the young population and the students.[3]

Clearly, for many MPs who have been appointed to the committees it would be expected not to possess many of the qualifications and skills that would be required for performing effective oversight. That is why additional staff and expertise on this issue is essential because it would support their performance. The Parliamentary Committee dealing with communication interception does not have additional staff members who would provide support in form of expertise to the Committee. Currently, there are only two persons who provide mainly administrative support to the Committee, but who are also working for the Committee for Supervising the Work of the Security and Counterintelligence Directorate and the Intelligence Agency.

Minchev who was chairman of the Committee supervising intelligence services in that time, reveals that information on usage of special investigative measures was lacking, although it has been promised to the MPs by the DSCI. Source: http://www.utrinski.mk/?ItemID=C42D9EC98F2D814B8C8A07A833CC73EC

This gap was to a certain extent supposed to be filled in by the establishment of the Parliamentary Institute, which is the Macedonian Parliament's way of providing greater resources and knowledge to Members of Parliament. Among Parliamentary Institute staff there is one person whose job portfolio lists "freedom and security", but there are also researchers covering "democracy and rule of law", "judiciary and human rights" and "contemporary political systems". The researchers do not have access to classified information so they cannot be expected to help the Committee overseeing interception of communications to analyze the documents received from the services. However, the MPs could rely on the Parliamentary Institute for legal analysis or comparative studies and this internal research body is yet to be utilized.

In addition, several international organizations (DCAF, NDI, Westminster Foundation) have offered training and support for the MPs in organization of oversight hearings, concrete themes in oversight or Europeanization in general; however, these have had very limited impact in their oversight activities.

A question that deserves greater attention is the lack of oversight culture and accountability, which because of the long inactivity among members of parliament has resulted in what appears to be resistance for more effective oversight. Such unresponsive approaches have become routine especially when it comes to the parliamentary committees overseeing the work of the intelligence services, including interception of communications. For example, probably one of the most experienced among all members in both committees overseeing the work of the intelligence services, Mr. Trajanov, has publically stated that the functioning of these committees is just for décor.

> *There is no real control of the security services anywhere in the world. Tell me an example of a Parliament that has such control! Yes, constitutionally and legally many countries have established forms and mechanisms for civilian control of the work and operative measures of the security services, but in practice, such control is little or not implemented at all. Especially in the segment of endangering human rights in case of implementation of*

measures such as surveillance and wiretapping. Hence, I believe that the control is reduced to being democratic décor.[64]

Mr. Trajanov's statement however is not far from the truth when one looks into the frequency of the meetings of the Committee for overseeing the use of communications interceptions. Only one meeting was recorded for 2014 and the status of the meeting is still "meeting in progress". In the whole of 2013 the Committee met also only once for the purpose of discussing its own annual report. In 2012 there is a somewhat better track record when the members of the committee met four times, mainly because the of the changes in the Law on interception of communications.[65]

Opposition parties play a crucial role in oversight in the Macedonian Parliament; mainly because through active scrutiny they hope to bring to the surface any wrongdoings by the party in power. Since the elections, in April 2014, the biggest opposition party SDSM has boycotted the work of the Parliament and does not participate of its work, blaming the ruling VMRO-DPMNE coalition for a series of irregularities affecting the outcome of the elections. This means that the Committees in the Parliament since April 2014 are composed primarily by members of ruling parties, making any active scrutiny over the interception of communication virtually impossible. Moreover the Committee on Oversight of Communications Interception has been structured in a way to provide greater scrutiny by appointing the Chairman of the Committee from the biggest opposition party. The boycott by the SDSM seriously hinders and further complicates any actual oversight activities. Even if hypothetically the opposition ends the boycott and returns to the Parliament, they would not be able to immediately restart overseeing the work of the security services, because the rules require vetting procedures of new Members first, which can take months.

Speaking about the vetting procedures, some challenges hampering

64 Katerina Blazevska. Контролата врз прислушкувањето еднаква на – нула! (The oversight of wiretapping is zero). 13.10.2014, DW. http://www.dw.de/контролата-врз-прислушкувањето-еднаква-на-нула/a-17989990?maca=maz-TB_maz_utrinski-5917-xml-mrss

65 Source: Parliament's website

oversight might also arise. In order to be granted access to classified information, the MPs should go under a vetting procedure that could take up to 6 months for top secret level. Moreover, in more complex cases the law envisages doubling this timeframe so the procedure could take up to a year.[66] In the past, there have been cases when prolonging of these procedures has obstructed committees' work.[67] Besides this, there are also other questions regarding the vetting process worth considering. Competent authority performing the vetting is the Directorate for Security and Counter-Intelligence. That is, the Directorate should give green light for those that should oversee its own work.

Enhanced types of scrutiny, such as unannounced field visits, asking for additional information from the institutions having the right to intercept communications, financial scrutiny including discussions about purposefulness of some of the investment in technology, have not been recorded, regardless of the political party in power (an exception is the "Campaign" case as described below). This goes hand in hand with the previously identified lack of oversight and accountability culture embedded in Macedonia's political elites. The opposition parties seem to run away from revealing scandals, which can be attributed to a private political agreement between the opposition party and the ruling parties, MPs expertise and capacity or even blackmail.[68]

66 Law on classified information, article 51
67 More information could be found at:
Andreja Bogdanovski, Strengthening intelligence oversight in Western Balkans – Macedonia as a case study, available at:
http://analyticamk.org/images/stories/files/report/macedonia_eng1.pdf
68 Saso Ordanoski, Journalist and political analyst (personal interview in Skopje, 15 January 2015.)

Politicization prevents oversight - Case "Campaign"

The only time when the Committee supervising interception of communications was handling a concrete case refers to the so-called "Campaign" case when the leader of the oppositional party "United for Macedonia" was sentenced to prison for the illegal financing of a pre-electoral campaign.

When the Committee was established in September 2011, after the parliamentary elections, it submitted a written request to the MoI to ask for information regarding usage of special investigative measures against Mr. Boskovski. When the Minister answered that the interception of communications measure had not been implemented in the particular case, the Committee decided to perform a field visit to the MoI in its full composition and request an insight into the documentation. This was followed by an answer that there is no documentation for interception of communications against Mr. Boskovski and that the MoI is open for visits by Mr. Petkovski (Chairman of the Committee) as it is for any citizen, he just has to specify the time and the reason for the visit. This was in a way surprising considering that a chairman or any other MP from an oversight committee clearly does not have the same status as a regular citizen interested in the work of the Ministry of Interior. Moreover, it seems that there are no considerations that field visits might also take place without prior announcement.

The Committee adopted a conclusion that the Parliament should consider the political responsibility of the Minister of Interior because of the degrading and irresponsible treatment regarding the Committee Supervising Communication Interception, MPs and the Parliament, as well as for the disrespect of the Law on Interception of Communications[4]. Mr. Petkovski was one of the initiators of an interpellation of the Minister, where among other things this was indicated as a reason for the interpellation. At the end, the interpellation was unsuccessful.

Apart from being an example of challenging communications between a Minister and a Committee, this case clearly indicates politicization as an important deficiency of parliamentary oversight. Besides the case itself, the rhetoric used by the Minister and the involved MPs was not freed from daily partisan bickering and fights for political points.[5]

5.3. OMBUDSMAN

In such a restricted environment where the Parliament is not in a position to produce tangible oversight results, it can be interesting to look for short to medium term solutions elsewhere. The Ombudsman can theoretically speaking fill the gap of the weak parliamentary oversight by exercising the powers vested in this position. For many years the Ombudsman has not shown any signs of interest into this matter, except in times of legislation changes, when he has been advocate of more precise and strict provision as guarantees of human rights and freedoms. However, the legal setup allows the Ombudsman to (among other things):

- Ask for clarifications and additional information from any state authorities;
- Enter into the premises of the state institutions (perform field visits);
- Request a meeting with an official/employee who can provide information about the case.[69]

Hence, in theory, the Ombudsman can perform field visits to the intelligence services with an aim to investigate any possible wrongdoings on this matter and meet in person the heads of these institutions and ask for accountability on particular cases regardless of the level of classification.

In the annual reports of the Ombudsman one could not find examples of concrete cases when citizens have submitted complaints on possible unauthorized wiretapping. However, the constitutional and legal positioning allows this independent institution to take more proactive approach. More precisely, article 13 from the Law on the Ombudsman says that the Ombudsman may initiate a procedure on his own initiative if he assesses that the constitutional and legal rights of citizens have been infringed. In addition, article 29 regulates that the Ombudsman shall follow the situation regarding the respect and protection of the constitutional and legal rights

69 Law on Ombudsman, Article 24

of citizen, inter alia, by means of visits and insights into the institutions.

This unused potential of the Ombudsman should be actively utilized in looking for files and court orders and checking whether the procedure in place has been respected, how this data is stored, whether the court orders are used only for the particular criminal act or may be misused for other purposes etc.[70] At the same time one needs to be cautions with the extent to which the Ombudsman in Macedonia can be proactive in this matter. Uranija Pirovska the Director of the Macedonian Helsinki Committee for Human Rights and longtime Public Relations officer at the Ombudsman's Office highlights the exposure of the Ombudsman to political pressures by knowing that it is the political parties who elect him/her. Also speaking of finances the Ombudsman is vulnerable to the range of activities and tools he/she can employ taking into account the source of finances for the work of the Ombudsman, being the state and upon approval by the Parliament. This can directly influence Ombudsman's independence and affect his performance.[71]

With the current setup the Ombudsman's powers are limited to recommending actions to be taken by authorities when any wrongdoings are recorded. In other words the Ombudsman does not have enforcement possibilities making his/hers recommendations dependent on the goodwill of state institutions. Past examples have shown that not in all cases do state institutions accept the Ombudsman's recommendations. However in cases such as illegal wiretapping where the right to privacy is directly challenged, due to the severity of infringement, his/hers recommendations and findings even though not enforceable cannot be ignored. This helps in adding a critical layer of pressure on state institutions.

70 Uranija Pirovska, Executive Director of Helsinki Committee for Human Rights (personal interview in Skopje, 23 January 2015.)
71 Ibid.

The case "Puc" as a challenge

The work of the Ombudsman when it comes to issues related to the work of the intelligence services received a new direction with the massive wire-tapping scandal "Puc" in 2015. After the main opposition party released materials claiming that more than 20 000 citizens of Macedonia have been under illegal surveillance by the Counterintelligence service, the Ombudsman on several occasions reacted through the media for as he says, blatant violation of human rights and expressed his concerns that the massive wiretapping is a terrifying phenomenon that will leave severe consequences to the society. He also questioned the existence of the right to privacy and legal certainty.[6] Even though during the first reactions, he had a position that "regarding general phenomena, the Ombudsman can express his concerns about the infringements of rights and call state institutions to respect rules and regulations, but there is nothing more within his mandate. He can open a case if an individual asks for protection"[7]; however, on 15.02.2015 the current Ombudsman Mr. Idzet Memeti started an investigation for a group of citizens upon his own initiative.[8] Later in March 2015 he started an investigation upon a complaint from a journalist for illegal wiretapping.

The results of the Ombudsman's efforts also depend on the cooperativeness of the institutions that are subject of investigation. The fact that the Ombudsman complained[9] that he was not able to obtain the necessary information from the Ministry of Interior and the Public Prosecution is worrying, especially because there are no legal obstacles for access to information. At the time of writing this policy paper, both cases are still in procedure.

6. CASE STUDY – ESTONIA

6.1. LEGAL FRAMEWORK

Interception of communications in Estonia is regulated within the broader framework for regulating the surveillance activities. In fact, there is a separate Surveillance Act that stipulates the rules for applying the measure, but no special attention is provided for the interception of commu-

nications as a more serious special investigative measure. Possible explanation for that is that there have not been major scandals with wiretapping as it was the case in most of the Balkan countries. In this context, the Surveillance Act lists surveillance activities such as covert collection of information, covert identification, covert examination and initial examination of documents and objects etc., including of information concerning the fact of messages being communicated via telecommunications networks, duration, manner and form of communication thereof and personal data and location of senders and receivers of such messages. In addition, the Security Authorities Act regulates restrictions on right to confidentiality of messages via examination of postal items and observing or recording messages and information transmitted over an electronic network or other means.[72]

While there are several state authorities competent for performing surveillance activities,[73] only the Police Board and Estonian Internal Security Service (equivalent to Macedonian Directorate for Security and Counterintelligence) are entitled to do wiretapping and recording of information.[74] They conduct such activities upon a written permission of a Prosecutor's Office or a preliminary investigation judge and the Criminal Code lists criminal offenses for which such measures could be applied. In the case of interception of communications for national security and defence purposes the permission is asked from an administrative court. The timeframe is more restrictive than the Macedonian one as the preliminary investigation judge grants permission for duration of two months with a possibility for a two-month extension. Both the Surveillance Act and the Criminal Procedure Code state that surveillance activities are permitted only if the desired purpose cannot be achieved in a manner which less violates the fundamental rights of persons. Interestingly enough, Estonian legislators decided to put into their law that "surveillance shall not be used in the interest of or

72 Security Authorities Act, article 25
73 Those authorities are: Security Police Board, Police Board, Tax Board, Board of Border Guard, Board of Customs, Prisons Department of the Ministry of Justice
74 Council of Europe, Reply to the questionnaire on special investigation techniques in relation to acts of terrorism: Estonia

to discredit political parties or political associations and movements."[75] The law also prohibits collecting and storing information concerning the beliefs of an Estonian citizen against his or her free will.

One of the most interesting practices in Estonia established by law is the obligation to notify the person with regard to whom surveillance activities were conducted and the persons whose private or family life was violated by these activities.[76] There are exceptions from this rule in case the notification could significantly damage rights and freedoms of other person, significantly damage criminal proceedings or confidentiality of methods, tactics of operation and equipment. The decision to not disclose the surveillance activities is made by the Public Prosecutor and is re-evaluated after certain period of time. The person who was subject of surveillance could examine the materials referring to him/her, including audio and video recordings.[77] Moreover, the person is informed about an appellant procedure and could submit a complaint or start court procedures against the authorities. All of the interviewees during the field research in Estonia agreed that the obligation for notification is one of the cornerstones of protection of human rights and liberties when performing surveillance activities. Moreover, every individual has the right to pose questions if he/she is the subject of surveillance.

It is also worth mentioning that the Surveillance Act has a separate section about liability for violation of this Act including provisions that employees of a surveillance agency or a person who has been recruited for surveillance activities who violates the established procedure, exceeds his or her authority or discloses or disseminates secret information shall bear liability.

Both crucial laws pay special attention to the control and oversight of the surveillance activities. They determine a special parliamentary commit-

75 Surveillance Act, Article 5
76 Surveillance Act, Article 17
77 Exception are information concerning private life of other persons, information which damages rights and freedoms of other persons, state secrets, information that could posses risk to the life and safety to other persons etc.

tee to conduct the oversight, but also the Prosecutor's Office exercises supervision. Moreover, the laws also envisage financial control over the financial resources allocated for surveillance. Financial supervision is performed by the Auditor General or an official of the State Audit Office designated by him/her and an official designated by the Minister of Finance.

6.2. SECURITY AUTHORITIES SURVEILLANCE SELECT COMMITTEE

The Estonian Parliament (Riigikogu) is an authorized oversight body through its specialized parliamentary committee called Security Authorities Surveillance Select Committee. The Committee performs oversight on whether the agencies comply with the legal obligations stemming from the Surveillance Act and other relevant laws.[78] All three relevant acts (Surveillance Act, Security Authorities Act and the Criminal Procedure Code) contain provisions on the supervision and oversight over the surveillance agencies provided by this committee.

The Prime Minister and a relevant minister shall inform the Committee of the activities of the security authorities and surveillance agencies and of the supervision over their activities, including submitting an overview of such matters, at least once in every six months.[79] In addition, the Committee has the right to summon persons and require documents for examination. So far, the MPs have not faced problems in terms of access to requested information. The only exception is the 3rd party rule[80] which means there

78 These include Constitution, State Secrets Act, Procedure for Registration and Disclosure of Persons who Have Served in or Co-operated with Intelligence or Counter-intelligence Organizations of Security Organizations or Military Forces of States which Have Occupied Estonia Act etc.

79 Security Authorities Act article 36

80 The "third party rule" refers to international exchange of classified information between the intelligence services where the services have an obligation not to disclose the received information to any third party without a permission from their source of information (the foreign intelligence service)

are limitations in regard to NATO secrets and international secrets.[81]

In general, the Committee performs random checks on the surveillance activities carried out in criminal proceedings or data collection proceedings that led to criminal proceedings. The checks generally focus on criminal cases in which a court ruling has been enforced. In addition, they control whether relevant court permission exists based on the log file reports received from the telephone operators. There is a clear mandate for the Committee for any detected criminal offense to submit it to the competent investigative body.[82]

One of the most interesting practices of this Committee is the frequency of meetings they have. Under the internal rules of the Parliament, each parliamentary committee shall have meetings twice a week. The Security Authorities Surveillance Select Committee convenes at least once a week and one more time during the same week if necessary.[83] Usually, twice a year (spring/autumn) they have the heads of the surveillance agencies present at the meetings. The Committee publishes its annual reports online where one can find comprehensive information on the work of the Committee. For instance, the annual report for 2013 shows that the Committee conducted numerous meetings with officials, including: meetings with the Prime Minister, the Minister of Defence, the Minister of Interior, Public Prosecutor, Director of the Tax and Customs Board, Director of the Police Board, representatives of the defence intelligence unit, representatives of the Ministry of Interior, Ministry of Defence and Ministry of Justice etc.[84] Moreover, the Committee informs on the content of each meeting, presenting concrete data when available such as statistical numbers in re-

81 Peep Aru, Chairman and Juri Nurme, Adviser of the Security Authorities Surveillance Select Committee of the 12th Riigikogu (Personal interview conducted in Tallinn, 12 November 2014)
82 Security Authorities Act, article 36
83 Peep Aru, Chairman and Juri Nurme, Adviser of the Security Authorities Surveillance Select Committee of the 12th Riigikogu (Personal interview conducted in Tallinn, 12 November 2014)
84 Annual review of the work of the Security Authorities Surveillance Select Committee for 2013

gards to surveillance activities and Committee's opinion on those numbers. In 2012, the Committee has discussed the Public Prosecutor's findings that the surveillance agencies have failed to notify citizens that had been subject of surveillance after the grounds for not-informing them have ceased to exist.[85]

Furthermore, the Committee carried out inspections comparing data received from telephone operators with the ones generated by the security authorities. The Committee relies on the methodology used by the Public Prosecutor when performing inspections.[86]

The Committee within the current mandate consists of a president, vice-president, six members and two advisors. The president of the Committee comes from the ruling parties and decisions are made by consensus. One of the features of all parliamentary committees is the lack of expertise among the MPs as they are all politicians with different backgrounds. However, within the Committee of the 12th Riigikogu,there is a former Minister of Interior in the current setting, which enables better oversight, but it is up to the political parties to appoint the committee members.[87]

Besides this committee, the National Defence Committee plays a certain role. Its role is very similar to the role of the Macedonian Committee on Defence and Security as its primary role relates to discussing draft legislation on defence and national security matters.

85 Annual review of the work of the Security Authorities Surveillance Select Committee for 2012
86 Ibid.
87 Peep Aru, Chairman and Juri Nurme, Adviser of the Security Authorities Surveillance Select Committee of the 12th Riigikogu (Personal interview conducted in Tallinn, 12 November 2014)

6.3. CHANCELLOR OF JUSTICE

The Chancellor of Justice (Ombudsman) has a strong position in Estonia as protector of human rights of the citizens. His/her primary role is dealing with complaints from the citizens on concrete cases, but is also actively engaged in the process of drafting and amending legislation where human rights infringements are possible.

Given the fact that it is an independent, constitutional body that have the public's trust more than most of other state bodies, its staff believe that the Ombudsman is more suitable to perform such oversight that the Parliament.[88] Therefore, there has been an initiative for strengthening this position and providing additional competences to exercise oversight of criminal legal procedures. Although the new competences are more symbolic than judicial, it is considered to send a strong message to the public that surveillance activities will be exercised in full compliance with the laws, creating confidence in the work of the agencies. One of the most important features is the clear competence of the Chancellor of Justice to act proactively, which was not the case previously and also better access to classified information.[89] The changes in the legislation take effect as of early 2015.

One of the drawbacks in the work of the parliamentary committees as an oversight mechanism is the lack of expertise among the MPs and lack of capable and sufficiently resourced staff. The Chancellor of Justice, on the other hand, is specialized in identifying human rights infringements and is freed from political influence. This Estonian institution employs people that have experience in working with surveillance agencies, which is a significant advantage in regards to necessary expertise.

The Chancellor of Justice aims at exercising control in these three areas:[90]

88 Mait Laaring, senior adviser; Raivo Aeg and Odyn Vosman, advisers to the Chancellor of Justice (personal interview conducted in Tallinn, 11 November 2014)
89 So far, the Chancellor of Justice had several restrictions in the access to classified information such as the 3rd party rule.
90 Mait Laaring, senior adviser; Raivo Aeg and Odyn Vosman, advisers to the

- Ensuring that the legislation is aligned with the Constitution and other laws;
- Ensuring that the legal provisions are lawfully implemented as envisaged;
- Ensuring that activities are conducted efficiently and purposefully.

While the criminal procedure surveillance entails different types of control and oversight (public prosecutor, judge), surveillance activities for intelligence purposes are different because there is no final court procedure. This means that judicial control is also very limited and therefore, it is of paramount importance to have proper additional control of this method of data collection.

Without a clear mandate to oversee surveillance activities, the Chancellor of Justice in Estonia has already acted proactively by lodging a constitutional review complaint with the Supreme Court elaborating the lack of effective mechanism for notification of all persons subjected to secret surveillance after completion of the activity. Not only has the Court agreed with the Chancellor of Justice and required improvements in the legislation, it also stood against Parliament's arguments regarding the costs, saying that if the State had enough money to conduct secret surveillance, it should also have enough to make sure that it is legal.[91]

Chancellor of Justice (personal interview conducted in Tallinn, 11 November 2014)
91 Source: Deputy Chancellor of Justice's speech "Ombudsman's role in the control of state's surveillance activities" at the Conference "Ombudsman's role in a democracy" in Tallinn, 19.09.2014.

6.4. BEST PRACTICES FROM ESTONIA IN RELATION TO MACEDONIA

The legal framework concerning the procedure for approval of surveillance activities including interception of communications is very similar to the Macedonian one – activities cannot be implemented without judicial approval. However, Estonian legislators provide stricter provisions in terms of timing meaning that the maximum duration of the measure is two months with a possibility for a two month extension. Macedonian laws allow interception of communications for up to four months in case of criminal cases and up to six months in case of endangering security and defence of the country (with adequate extension if needed). One cannot argue which approach is better. The length of application should be suitable to cover the needs for collecting sufficient evidence, but longer interceptions significantly increase the risk of human rights infringements especially in cases where the application of the measure have not led to criminal procedure.

One of the most interesting practices established by law is the obligation for Estonian state authorities to notify the person who had been subject of surveillance. Such practice could have a positive influence in terms of better selectivity for the application. Knowing that the person will be notified afterwards would likely discourage state institutions from requesting such special investigative measures when the grounds of suspicion are weak.

Regarding parliamentary oversight, the differences in terms of (in)activity between the Macedonian and Estonian committees are evident. While Macedonian Committees tasked to oversee intelligence rarely meet more than a few times per year, their Estonian colleagues convene every week. As seen from the above section dedicated to the Macedonian Parliament, there are indeed objective and subjective limitations impeding proper oversight. Given that the function of MP shall be performed professionally,[92]

92 Law on the Parliament, article 7

the importance of a more proactive approach should be acknowledged.

In addition, the Estonian legal framework enables a better operating environment for parliamentary committees, having better developed mechanisms for oversight in the primary legislation. State authorities report to the Parliament more frequently and the oversight Committee has powers to summon persons and request documents for examination. Another good practice can be found in the transparency of the Estonian Security Authorities Surveillance Select Committee. Its annual reports are available online and contain information of all activities throughout the year, including information on the nature and results of meeting with state officials (Prime Minister, ministers of justice, internal affairs and defence, directors of police, tax administration and customs etc.). This is especially important because such meetings take place behind closed doors due to confidentiality.

Finally, the limitations of parliamentary oversight such as lack of expertise and politicization are acknowledged by the stakeholders in Estonia. Therefore, the efforts to strengthen the position of their Ombudsman (called Chancellor of Justice) deserve closer attention. The Macedonian Ombudsman already has similar or even stronger competences, such as the ability to act upon his/her own initiative and has access to state institutions' premises and documentation.

7. CONCLUSION

This paper aimed to assess the current Macedonian legislative framework for intercepting communications, to detect possible gaps enabling violation of human rights and civil liberties and to provide recommendations for better oversight and control of the institutions authorized for its implementation.

The area of interception of communications is regulated by several laws and all of them faced important changes in the last few years. The Law on Criminal Procedure provides the general framework while specific provisions could be found in the Law on Interception of Communications. Since the end of 2013, the Public Prosecutor, who submits the requests for interceptions for approval to the competent court, plays a major role in the whole procedure. Although there are four institutions authorized to implement such measures (the Ministry of Interior, Ministry of Defence, Financial Police and Customs Administration), the Ministry of Interior is arguably the most important actor in terms of competences and capacities.

Statistical data reveals a worrying trend that the courts are completely aligned with the Ministry of Interior, when interceptions of communications are requested. With a rate of 100% approvals, Primary Court Skopje 1 has not found any request for interceptions to be inadequate. Questions are raised regarding the expertise of the judges to assess potential security threats and grounds for suspicions, but there are also concerns about the independence and impartiality of the judicial power.

In regards to parliamentary oversight, the legal framework is largely in place – having parliamentary committees specialized in overseeing interception of communications is rare to find even in the most developed democracies. Nevertheless, existing mechanisms are dysfunctional in practice. Lack of political will, accountability culture and access to expertise among the MPs does not enable proper oversight of the authorized institutions. Moreover, frequent and deep political crises prevent even the formation of the committee and the conduct of basic oversight. The Ombudsman also has certain powers to oversee the work of security sector institutions; so

far, they are underutilized as the Ombudsman mostly focuses on concrete complaints by the citizens.

On the other hand, the Estonian Security Authorities Surveillance Select Committee has a surprisingly high frequency of meetings – at least once per week and well established dialogue with all state institutions that have surveillance powers. However, deficiencies in this model have also been identified resulting in Estonian legislators considering vesting more powers in the Ombudsman as an independent controlling institution.

RECOMMENDATIONS:

These recommendations refer to the shortcomings identified in the analysis and do not aim to offer suggestions in resolving the political crisis as a result of the massive wiretapping scandal "Puc".

OMBUDSMAN

- The Ombudsman institution in Macedonia should more actively utilise its authorisations in conducting oversight of communications interception. It should especially make use of its powers to act proactively upon questions of public interest.
- The Law on the Ombudsman should be amended with provisions providing a clearer mandate of the Ombudsman's role in communications interception oversight.
- The Ombudsman's office would benefit from employing additional staff who can provide expertise in intelligence oversight (including communications interception).

PARLIAMENT

- The legal framework should be developed further in order to regulate the mandate of the parliamentary committees and to define the mechanisms at their disposal in a clear and precise manner. This includes establishing a relationship with the intelligence services, further regulating field visits to the intelligence services (announced or unannounced and composition of the working group to be determined) and oversight hearings.
- The ability to ask for specific reports or information throughout the year should also be regulated, establishing the procedure for requesting additional information and deadlines for the services to

provide what has been requested.

- The Rules of Procedures of the Parliamentary Committees tasked to oversee the work of the intelligence services and the interception of communication should also be amended including a minimum number of meetings quota, for example once in a month. This way, the Committee will ensure continuity in its work and the MPs will establish regularity in their activities.

- When proposing new members for oversight committees, political parties should be aware of their personal affinities, and consider their knowledge, experience and capabilities for performing such duties. The political will and the individual's will and ability are important factors affecting the performance of adequate oversight.

- MPs should regularly utilize the Parliamentary Institute as an internal research body. Their input could be used to provide comparative and other type of analysis from perspective of law, human rights, state security etc. Apart from the Parliamentary Institute, MPs can also benefit from support coming from civil society organizations (think tanks) which specialize in this area.

- Committee members should discuss annual reports of the Public Prosecutor submitted to the Parliament, especially taking into consideration their comprehensiveness as defined by the Law on Criminal Procedure. Additionally, the committees should establish regular cooperation with the Public Prosecution, inviting the State Public Prosecutor to committee meetings.

- Committee members should also establish cooperation with independent oversight institutions such as the Ombudsperson and invite him/her at Committee meetings.

- Committees tasked to oversee the legality of communications interceptions should also be allowed to perform oversight of telecommunications operators.

OTHER INSTITUTIONS:

- Employees within the Ministry of Interior, Ministry of Defence, Customs Administration and Financial Police should undergo training and attend seminars to become more familiar with the concept of oversight and accountability and its value to a democratic society.

- Public prosecutors and judges should undergo specialised trainings to better understand the work of the institutions that implement special investigative measures so they can better assess the necessity of particular measures in a concrete case. In some cases, less invasive measures are available to obtain equal results.

BIBLIOGRAPHY

Legislation

Law on interception of communications, Official gazette of the Republic of Macedonia no. 121/2006, with amendments O.G. 110/2008, 116/2012

Law on electronic communications, Official gazette of the Republic of Macedonia no. 39/2014, with amendments O.G. 188/2014

Law on criminal procedure, Official gazette of the Republic of Macedonia no. 15/1997 with amendments O.G. 44/2002, 74/2004, 83/2008, 67/2009 (out of legal force)

Law on criminal procedure, Official gazette of the Republic of Macedonia no. 150/2010, with amendments O.G. 51/2011, 100/2012

Law on internal affairs, Official gazette of the Republic of Macedonia no. 42/2014, with amendments O.G. 116/2014, 33/2015

Law on Defence (Consolidated text), Official gazette of the Republic of Macedonia no. 185/2011

Law on Customs Administration, Official gazette of the Republic of Macedonia no.46/2004, with amendments O.G. 81/2005, 107/2007, 103/2008, 64/2009, 105/2009, 47/2010, 158/2010, 53/2011, 113/2012, 43/2014, 167/2014, 33/2015

Law on financial police, Official Gazette of the Republic of Macedonia no. 55/2007 (out of legal force)

Law on financial police, Official Gazette of the Republic of Macedonia no. 12/2014, with amendments O.G. 43/2014, 33/2015

Law on the Parliament of the Republic of Macedonia, Official Gazette of the Republic of Macedonia no. 104/2009

Law on the Ombudsman of the Republic of Macedonia, Official

Gazette of the Republic of Macedonia no.60/2003, with amendments O.G. 114/2009

Law on classified information, Official Gazette of the Republic of Macedonia no.9/2004, with amendments O.G. 113/2007, 145/2010, 80/2012, 41/2014

Security Authorities Act , RT I 2001, 7, 17

Rules of Procedure of the Committee for supervision of measures for interception of communications by the Ministry of Interior and Ministry of Defence

Council of Europe, European Convention on Human Rights as amended with Protocols no. 11 and 14 and supplemented by Protocols no. 1, 4, 6, 7, 12 and 13

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

OTHER DOCUMENTS AND REPORTS:

Annual report for the work of the Public Prosecution of the Republic of Macedonia for 2010

Annual report for the work of the Public Prosecution of the Republic of Macedonia for 2011

Annual report for the work of the Public Prosecution of the Republic of Macedonia for 2012

Annual review of the work of the Security Authorities Surveillance Select Committee for 2012

Annual review of the work of the Security Authorities Surveillance Select Committee for 2013

Council of Europe, Reply to the questionnaire on special investigation techniques in relation to acts of terrorism: Estonia

Court of Justice of the European Union PRESS RELEASE No 54/14, The Court of Justice declares the Data Retention Directive to be invalid, Luxembourg, 8 April 2014

Deputy Chancellor of Justice's speech "Ombudsman's role in the control of state's surveillance activities" at the Conference "Ombudsman's role in a democracy" in Tallinn, 19.09.2014.

European Commission's Data Retention Experts Group, Statistics on Requests for data under the Data Retention Directive, available at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf

European Commission, Evidence for necessity of data retention in the EU, March 2013

European Commission Progress Report on Macedonia for 2011

European Commission Progress Report on Macedonia for 2014

Claire Fransoice ECJ's Invalidation of EU Data Retention Directive Creates Confusion Over Telecommunications Service Providers' Data Retention Obligations, Privacy Law Watch, 13.05.2014, available at: http://www.hunton.com/files/Publication/dec9c9bc-0527-4620-9664-ab40152923be/Presentation/PublicationAttachment/39d39846-4efd-473d-81da-ea264b-fbb90d/ECJs_Invalidation_of_EU_Data_Retention_Directive.pdf

Strategic plan of the Customs Administration 2013 – 2015

Strategic plan of the Customs Administration 2014 – 2016

T-Mobile Macedonia suggestions to the draft Law on electronic communications. https://ener.gov.mk/default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=kD/JU8uL687IkYMWVEaxNw

VIP Macedonia suggestions to the draft Law on electronic communications. https://ener.gov.mk/default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=kD/JU8uL687IkYMWVEaxNw p.27

PUBLICATIONS:

Andreja Bogdanovski, "Chapter: Macedonia" in *Almanac on Security Sector Oversight in Western Balkans,* ed. Franziska Klopfer and Douglas Cantwell with Miroslav Hadžić and Sonja Stojanović (Belgrade Center for Security Policy Geneva and Centre for the Democratic Control of Armed Forces, 2012) 129 - 156

Andreja Bogdanovski, *Strengthening intelligence oversight in Western Balkans – Macedonia as a case study* (DCAF, 2012)

Andreja Bogdanovski and Magdalena Lembovska, *Towards 2nd generation of Security Sector Reform in Macedonia* (Analytica think tank, 2012)

Jovan Bliznakovski and Misha Popovic, *Public opinion on "Wiretapping" affair,* (Macedonian Center for International Affairs & Institute for Democracy Societas Civilis Skopje, 2015)

Magdalena Lembovska, *Comparative analysis of regional practices for financial parliamentary oversight of intelligence services* (Analytica think tank, 2013)

Bojan Marichikj and Ljupcho Petkovski, *The political culture, Europeanization, and fears in Macedonia* (Macedonian Center for European Training, 2014)

MEDIA:

Goran Adamovski, Што содржи извештајот на УБК до Парламетот? (What is included in the DSCI's report to the Parliament?, Utrinski daily, 15.05.2012, last accessed 18.05.2015, available at: http://www.utrinski.

mk/?ItemID=C42D9EC98F2D814B8C8A07A833CC73EC

Katerina Blazevska, Контролата врз прислушкувањето еднаква на – нула! (The oversight of wiretapping is zero). DW, 13.10.2014, last accessed 18.05.2015, available at:

http://www.dw.de/контролата-врз-прислушкувањето-еднаква-на-нула/a-17989990?maca=maz-TB_maz_utrinski-5917-xml-mrss

Frosina Dimeska, Обвинителот чека пријава, Правобранителот загрижен [The Public Prosecutor waits for criminal complaint, the Ombudsman is worried,] Radio Slobodna Evropa, 16.03.2015, last accessed 18.05.2015, available at: http://daily.mk/makedonija/obvinitelot-cheka-prijava-pravobranitelot-zagrizhen

Опозицијата решена преку Собранието да ја контролира Владата [Opposition determined to control the Government through the Parliament], Kapital, 05.07.2012, last accessed 23.12.2014, available at: http://www.kapital.mk/MK/makedonija/86076/opozicijata_reshena_preku_sobranieto_da_ja_kontrolira_vladata.aspx

Одговорноста на Јанкуловска пред пратениците [Jankulovska's responsibility in front of the MPs], Nova Makedonija, 23.12.2011, last accessed 18.05.2015, available at: http://daily.mk/makedonija/odgovornosta-na-jankuloska-pred-pratenicite

INTERVIEWS:

Peep Aru, Chairman and Juri Nurme, Adviser of the Security Authorities Surveillance Select Committee of the 12th Riigikogu (Personal interview conducted in Tallinn, 12 November 2014)

Aivar Engel, Adviser/Head of Secretariat of the National Defence Committee (personal interview conducted in Tallinn, 12 November 2014)

Gordan Kalajdziev, Professor at the Faculty of Law Skopje (personal

interview conducted in Skopje, 24 December 2014)

Mait Laaring, senior adviser; Raivo Aeg and Odyn Vosman, advisers to the Chancellor of Justice (personal interview conducted in Tallinn, 11 November 2014)

Saso Ordanoski, Journalist and political analyst (personal interview conducted in Skopje, 15 January 2015)

Uranija Pirovska, Executive Director of Helsinki Committee for Human Rights (personal interview conducted in Skopje, 23 January 2015).

Interview with an Official from the Ministry of Interior (personal interview conducted in Skopje, 27 January 2015)

(Table Endnotes)

1 Bojan Marichikj and Ljupcho Petkovski, The political culture, Europeanization, and fears in Macedonia, Macedonian Center for European Training, 2014 pg. 35

2 Macedonian Center for International Affairs and Institute for Democracy Societas Civilis Skopje

3 Jovan Bliznakovski and Misha Popovic, Јавното мислење за аферата прислушување [Public opinion on "Wiretapping" affair], Macedonian Center for International Affairs & Institute for Democracy Societas Civilis Skopje, 2015

4 Одговорноста на Јанкуловска пред пратениците [Jankulovska's responsibility in front of the MPs], Nova Makedonija, 23.12.2011, available at: http://daily.mk/makedonija/odgovornosta-na-jankuloska-pred-pratenicite

5 Source: stenographic notes available at www.sobranie.mk

6 Source: A1 On "Memeti: I strongly commend the wiretapping, this is a blatant violation of human rights", 10.02.2015

7 Source: Radio Free Europe "The Public prosecutor waits for a complaint, the Ombudsman is worried", 10.02.2015, available at: http://daily.mk/makedonija/obvinitelot-cheka-prijava-pravobranitelot-zagrizhen

8 Information received from the Ombudsman's Office

9 Source: Vest "Memeti: The Public Prosecution and the Ministry of Interior do not provide information on the massive wiretapping", 21.05.2015

ABOUT THE AUTHORS

Andreja Bogdanovski works as a Security Research Fellow at Analytica think tank in Skopje, Macedonia since 2009. He is an author of several studies relating to the democratic governance and reforms of the security sector in Macedonia. Mr. Bogdanovski has completed a Master's degree in International Peace and Security from the Department of War Studies at King's College London. His interests include: international security, political risk assessment, de-facto states, security sector reforms, intelligence governance and other. Prior to joining Analytica Andreja worked as a project manager at the British Council in Macedonia (2007-2008).

Magdalena Lembovska is a Research Fellow on the Security Policy Programme at Analytica Think Tank since 2012. Her work focuses on researching contemporary security issues and the concept of good governance. Ms Lembovska has authored several policy papers in the field of security sector reform with focus on oversight and control. She has studied political science followed by a master program in security and financial control in Skopje, Macedonia.

COMMUNICATIONS
INTERCEPTION OVERSIGHT
IN MACEDONIA

"Making The Impossible Possible"

Andreja Bogdanovski
Magdalena Lembovska

Skopje, 2015