Oversight and Transparency in the Canadian Intelligence Establishment: **Lessons for a Young Democracy**

Natasia Kalajdziovski

LIST OF ABBREVIATIONS

ATIP	Access to Information and Privacy Section
CFIC	Canadian Forces Intelligence Command
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence (Canada)
RCMP	Royal Canadian Mounted Police
RCMP SS	Royal Canadian Mounted Police Security Service
SIGINT	Signals intelligence
SIRC	Security Intelligence Review Committee

| INTRODUCTION

Intelligence as statecraft has been a long-practiced and embraced manner for nation-states to gather information about both their enemies and allies in equal measure. However, as intelligence practice has become more formalised throughout the past century, new expectations relating to the openness and transparency of intelligence actors – especially those operating in liberal democratic states – came to the fore. There is now an expectation of acknowledgement from intelligence actors toward their populaces about their mandates, purpose, and activities; this is accomplished through both greater efforts at transparent dialogue between the two bodies, but also through comprehensive oversight mechanisms – mechanisms which are put in place to ensure that the activities of intelligence actors remain within their legislative remit and within the law.

However, for young and emerging democracies – particularly those with a post-communist legacy – finding the right balance between security and openness can be difficult. The implementation and enforcement of effective and robust oversight mechanisms for a young security establishment can bring with it unique challenges, especially in light of increasingly diverse defence and security concerns. Such challenges have recently surfaced in the security establishment of the Republic of Macedonia, where February 2015 revelations put forward by Macedonia's largest opposition party alleged widespread illegal wiretapping of more than 20 000 individuals in contravention of legislation governing communications intelligence.[1] In light of this, questions regarding the effectiveness of the current oversight structure have since entered into the national security narrative.

As such, the aim of this report will be to examine the oversight mechanisms and transparency structures – strengths and weakness alike – of a well-established liberal democratic state in order to glean lessons applicable to a young democracy. In this effort, the Canadian security establishment will be employed as a comparative case, as it offers insight into a well-established and legislatively-grounded intelligence culture. The report will first give a brief organisational overview of the main intelligence actors in Canada; this will be followed by an outline of any oversight mechanisms and transparency structures in place, with a subsequent analysis of their effectiveness. Finally, the report will offer lessons and best practices which can best be applied to Macedonia.

| ORGANISATIONAL OVERVIEW

Similarly to its allies, Canada enjoys a comprehensive security establishment that strives to meet the needs of various security realities and provide actionable intelligence product to the Government of Canada and its associated ministries. Most importantly, it is the kind of establishment which understands the necessity of balanced openness about its various mandates and roles in Canadian society; this is reflected in the establishment's numerous efforts to make itself more transparent, whilst continuing to keep in line with its defence priorities.

[1] For further discussion on the allegations, and for a lengthy analysis of communications interception oversight in Macedonia, please see: Andreja Bogdanovski and Magdalena Lembovska. *"Making the Impossible Possible": Communications Interception Oversight in Macedonia.* (Skopje: Analytica, 2015).

For the purposes of identifying the strengths and weaknesses found in the establishment's oversight mechanisms, this report will focus predominantly on Canada's two civilian intelligence agencies: the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE).

I. Canadian Security Intelligence Service (CSIS)

Perhaps the most well-known of these civilian services is CSIS. The Service was created in 1984 through the *Canadian Security Intelligence Service (CSIS) Act*, an act of legislation put in place to replace CSIS' scandal-plagued predecessor, the Royal Canadian Mounted Police Security Service (RCMP SS). Due to the paramilitary nature of the RCMP, and the issues which arose with housing the country's primary intelligence service therein, CSIS was created under the auspices of intelligence demilitarisation. Thus, CSIS became Canada's first civilian intelligence agency. Between 1984 and 2015, CSIS' mandate remained virtually untouched; however, this changed with the introduction and passing of Bill C-51 earlier this year, which is set to vastly expand CSIS' collection powers. The implications of this will be discussed further in the latter sections of this report.

In regards to governmental responsibility, CSIS must report to Parliament through the Minister of Public Safety, and its current modus operandi focuses predominantly on intelligence gathering and counter-terrorism. Importantly, the *CSIS Act* stipulates that while the Service retains the right to investigate individuals or organisations "suspected of engaging in activities that may threaten the security of Canada", its reach does not lawfully extend to acts such as protests, dissent or advocacy unless they are "linked to threats to Canada's national security".[2]

II. Communications Security Establishment (CSE)

Whereas CSIS is involved in a broader spectrum of intelligence responsibilities, Canada's CSE is predominantly responsible for the collection, analysis and dissemination of foreign signals intelligence (SIGINT). Additionally, as defined in the *National Defence Act*, the mandate of CSE extends to the securitisation and protection of Canadian communications.[3] Unlike the organisational youthfulness of its counterpart, CSE has existed in some form since 1941, when it was known as the Examination Unit; however, it only came under the purview of the Department of National Defence (DND) in 1975.[4]

Currently, the organisation is responsible to the Minister of National Defence through the CSE Chief; the Minister is then accountable to Parliament. CSE receives its instructions via Ministerial Directive, and the actions it undertakes can only be conducted within both the aforementioned directives and previously established Canadian law.[5]

[2] Bill C-23. *Canadian Security Intelligence Service Act*. Parliament of Canada, RSC 1985. Amended 25 April 2015.

[3] Bill N-5. *National Defence Act.* Parliament of Canada, RSC 1985. Amended 1 June 2015.

[4] Previous to 1974, the existence of CSE was a governmental secret; after its public exposure through a documentary from the Canadian Broadcasting Corporation, it came under the mandate of the DND. "Communications Security Establishment – History". Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/history-histoire

[5] "Communications Security Establishment – What We Do and Why We Do It". Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/inside-interieur/what-nos

III. Non-Civilian Intelligence Actors

While CSIS and CSE are the predominant intelligence agencies in the Canadian security establishment, it is important to note the non-civilian agencies with legislative jurisdiction in the realm of intelligence – most notably, the RCMP and the Canadian Forces. For the latter, that responsibility resides within the Intelligence Branch of the Forces, under the Canadian Forces Intelligence Command (CFIC). From its five collection bodies,[6] it provides all-source analysis for both its own operational purposes and to meet the needs of the DND. Additionally, although most of the national intelligence responsibilities were stripped away through the *CSIS Act*, the RCMP does still retain an intelligence capacity through three units within their Specialised Operational Services section,[7] found within their National Division. However, this capacity is limited and is used within a different remit to that of CSIS.

Although the analysis of oversight mechanisms will focus on the civilian agencies within the security establishment, it is still important to view and understand these agencies within the context of the greater intelligence picture in Canada.

| OVERSIGHT MECHANISMS AND TRANSPARENCY

In an effort to determine the effectiveness and comprehensiveness of the oversight and transparency culture of the Canadian security establishment, this section will outline both CSIS and CSE's committed oversight bodies – their mandate, purpose and composition – to better understand their relationship to the agencies which they monitor. Additionally, this section will delineate any efforts or programmes put in place to further build trust and openness with the Canadian public at large.

I. CSIS and the Security Intelligence Review Committee (SIRC)

Of all the bodies that hold some kind of intelligence capacity in the Canadian security establishment, CSIS provides the most comprehensive efforts at increased transparency. While both CSIS and CSE have singularly responsible legislative bodies mandated with oversight responsibilities, it is the founding of CSIS in a culture dedicated to greater openness which renders it unique in this respect.

As mentioned previously, upon its foundation CSIS became Canada's first civilian intelligence agency. The move toward this formulation came through the recommendations put forward by two federal commissions – the MacKenzie Commission, and later the McDonald Commission[8] – that were tasked, broadly speaking, with identifying the organisational ineffectiveness of the

[6] These are as follows: the Canadian Forces Joint Imagery Centre; the Canadian Forces National Counter-Intelligence Unit; the Joint Meteorological Centre; the Mapping and Charting Establishment; Joint Task Force X.
[7] These are as follows: the Divisional Criminal Analysis Unit; the Criminal Intelligence Unit, and; the Criminal Intelligence Information Exchange Unit.
[8] "Security Intelligence Review Committee – Looking Back". SIRC. Accessed July 2015 http://www.sirc-csars.gc.ca/opbapb/rfcrfx/sc02a-eng.html

RCMP SS. Critically, both recommended a separation of intelligence powers from the RCMP; they acknowledged that under the current system, the "problem of balancing the need for accurate and effective security with the need to respect democratic rights and freedoms could not be adequately resolved".[9]

In addition to the *CSIS Act* creating the Service, it in tandem introduced CSIS' main oversight body: the Security Intelligence Review Committee (SIRC).[10] The SIRC is comprised of members who are appointed –after consultation by the Prime Minister and the Leaders of the Opposition – by the SIRC's Governor-in-Council. The key point in this system of appointment resides in the fact that all members of the Committee must also be members of the Privy Council – membership of which grants security clearance to highly classified information.[11] Moreover, in its pursuit of comprehensive analysis, the Committee is granted access to all CSIS-related documents and reports, save Cabinet Confidences.

After completing their review, the Committee must then send an annual report to CSIS' responsible ministry; this is done in addition to special reports which the Committee undertakes – usually relating to extraordinary topics or controversies[12] – as well as situational briefs, departmental performance reports, and financial/expenditure statements. These reports are available for public consumption,[13] although they may have redacted elements due to security concerns.

II. CSIS and Further Mechanisms for Transparency

There are two legislative acts which govern public access to information related to CSIS: the *Privacy Act* and the *Access to Information Act*. The former pertains specifically to the personal information of individuals, whereas the latter deals with more general records that are under the control of federal governmental institutions.[14] Both provide individuals[15] with the right to make formal requests for information, and these requests are handled by CSIS' "Access to Information and Privacy" (ATIP) section. The section "processes formal requests under the *Acts*, responds to consultations received from other government institutions and handles complaints lodged with

[9] "Canadian Security Intelligence Service – History of CSIS". Government of Canada. Accessed July 2015 https://www.csis.gc.ca/hstrrtfcts/hstr/index-en.php

[10] The *Act* also introduced the Office of the Inspector General, but this office was dissolved by governmental order in 2012 and its responsibilities were absorbed into the SIRC.

[11] This clearance is not extended to all parliamentarians.

[12] See, for example: "CSIS' Role in the Matter of Omar Khadr"; "Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar", etc.

[13] The annual reports can be found here: http://www.sirc-csars.gc.ca/anrran/index-eng.html

[14] "Canadian Security Intelligence Service – Access to Information and Privacy Section". Government of Canada. Accessed July 2015 https://www.csis.gc.ca/tp/index-en.php

[15] Through both *Acts*, Canadian citizens, permanent residents, and individuals present in Canada can make information requests; however, only the *Access to Information Act* grants corporations present in Canada the right to make an information request. Additionally, it is free to make a request through the *Privacy Act* even if you are a Canadian citizen living abroad, and the request can easily be made online. However, a $5.00CAD charge is applicable to requests made under the *Access to Information Act*.

the Information and Privacy Commissioners",[16] and is indicative of the Service's desire to formally commit to greater openness and transparency.[17]

In addition to its legislative responsibilities regarding access to information, CSIS has also introduced four programmes in an effort to bolster its transparency and public accountability:

1) Public Liaison and Outreach Programme:
    - Purpose is to educate the general public about CSIS' mandate, function in the security establishment, and greater role in society
    - Disseminates CSIS-related material and publications through its *Public Report*, issues backgrounders, multimedia presentations, etc.
2) Liaison/Awareness Programme:
    - Focus is on issues relating to economic espionage; aims to educate through ongoing dialogue with private and public organisations
3) Media Relations Programme:
    - Liaison body between the Service and media bodies tasked with providing timely information for public consumption via the media
4) Cross-cultural Roundtable on Security[18]
    - Forum created with the aim of "engaging Canadians in a long-term dialogue on national security matters, recognising that Canada is a diverse and pluralistic society"; is part of Canada's broader *National Security Policy*

Broadly-speaking, these programmes are aimed at educating the general public about CSIS activities, and to have said public engage in discourses relating to security issues and approaches to safety. Additionally, there is an impetus on presenting security as a national concern, in which individual citizens can play a role and lend their voice in dialogue.

III. CSE and the Office of the CSE Commissioner

Like its counterpart, CSE also has a singular body responsible for oversight over its activities and investigating any suggestions of operational wrongdoing. The Office of the CSE Commissioner is a fully independent body from Parliament, which makes it unique in comparison to the SIRC; the position of Commissioner must be held by a supernumerary or retired judge of superior court – not a member of the Privy Council.[19] The Office is expected to make two different kinds of

[16] "Canadian Security Intelligence Service – Access to Information and Privacy Section".

[17] Additionally, the summaries of all completed (and declassified) information requests made to the Government of Canada since January 2012 are available online in a searchable database, and can be requested for viewing at: http://open.canada.ca/en/search/ati. Information requests made relating to CSE and the RCMP can be found here, as well as requests relating to other security-responsible bodies in the Canadian security establishment.

[18] "Public Safety Canada – Connecting with Canadian Communities: Cross-Cultural Roundtable on Security". Government of Canada. Accessed July 2015 http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crss-cltrl-rndtbl/index-eng.aspx

[19] "Communications Security Establishment – How is CSE Held Accountable?" Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/inside-interieur/review-examen

reports: one classified, for consumption by the Minister of National Defence,[20] and; one public annual report, summarised for Parliament.[21]

All reports – and the recommendations found therein – must be responded to in writing from the CSE Chief via the Minister; since 1997, 150 recommendations have been made, with 93% having been acted upon.[22] The Office also has comprehensive powers in regards to access to information in compiling its analysis for report publication. It has full access to all classified information and to all organisational staff; additionally, under Part II of the *Inquiries Act*, the Commissioner has "the power of subpoena, and the power to summon witnesses to give evidence under oath or solemn affirmation".[23] According to the Office, to date it "has not found any of CSE's activities to be unlawful".[24]

IV. CSEC and Further Mechanisms for Transparency

Given the recent Edward Snowden-related controversy over the alleged ambiguous morality present in the collection of SIGINT by western governments, CSE has made a significant effort to remain very transparent about the ethics through which it operates. In this respect, the organisation has provided a detailed discussion on its website regarding the established Ethics Charter to which it has developed for its purposes and to which it adheres, outlining its own – and its employees' – expected behaviours, lawful conduct, and integrity.[25] In relation to this, it also provides links to relevant policies and guidances, such as legislation and governmental bodies to which CSE is expected to adhere and to submit.[26] Most importantly, however, it outlines administrative and disciplinary measures inherent in prosecuting behaviours or actions contradicting those outlined in the Ethics Charter, and instructions on how to disclose instances of wrongdoing.

V. Effectiveness of Mechanisms and Controversies

Overall, the efforts and various programmes put in place by both CSIS and CSE to remain transparent are comprehensive, clear, and implemented in goodwill. The culture of transparency and openness that defines the organisational aspects of the Canadian security establishment should be understood as one of its greatest strengths, particularly in its desire to build genuine trust and respect amongst the population which it strives to protect. In particular, CSE's defined code of ethics and CSIS' outreach programmes are of key importance in organisational openness.

[20] This is an annual report, but the Office can also create specialised reports based on departmental requests. However, these fall under the remit of the Minister, and are thus classified.

[21] The summary report includes a summary of the annual private report that is disseminated to the Minister, as well as any specialised reports which have been requested throughout the year.

[22] "Communications Security Establishment – How is CSE Held Accountable?"

[23] *Ibid.*

[24] *Ibid.*

[25] "Communications Security Establishment – CSE Ethics Charter". Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/about-apropos/ethics-charter

[26] Some of these bodies include: Privacy Commissioner of Canada; Auditor General; Information Commissioner' Canadian Human rights Commission, and; Commissioner of Official Languages.

However, when it comes to the structures which govern the oversight of the Canadian security establishment, criticisms have been levied which suggest that the comprehensiveness of these structures does not go far enough. Generally speaking, the biggest issue identified is that mechanisms for accountability have not been propped up in tandem with expanding security powers, particularly since 9/11. The prime example of this is the composition of the SIRC and the Office of the CSE Commissioner; while these appear, in theory, to be effective mechanisms for oversight, the issue resides in the fact that their compositions have remained largely unchanged since their creation – 1984 for the former, and 1996 for the latter.[27] Simply put, as security powers and strategic coverage have widened, the bodies responsible for oversight have remained stagnant, thus inhibiting their effectiveness.

Additionally, the legislative bodies which are responsible for intelligence oversight do not have the appropriate remit to deal with the subject matter inherent in such analysis. For example, there are two parliamentary standing committees in which issues of intelligence and security are discussed: one in the House of Commons, and one in the Senate. However, the remit of these committees is broad – "defence", generally – and the members of the committees do not have security clearance; as such, they cannot report on issues of oversight in any effective way.[28] Moreover, there is no Cabinet-level committee on national security – one to act as a broad cross-agency review body and to compliment the work done by the singular review bodies responsible for agency oversight – which hinders the robustness of intelligence accountability.

The aforementioned issues have been exasperated by the introduction of Bill C-51 – the so-called Anti-Terrorism Bill – which, broadly-speaking, will grant greater power to the intelligence services and proposes more robust intelligence-sharing between the various agencies responsible for defence and security. Although a number of critiques have been brought forward by legal and intelligence experts (as well as human rights and civil liberties groups, and former prime ministers[29]) this report will iterate just one aspect: that C-51 fails to provide appropriate oversight expansion in tandem with the expansion of powers, and that an already-ailing system will become even more ineffective.

This phenomenon – the disjoint between expanding security powers and stagnant oversight mechanisms – should be understood as an issue of lack of political will, rather than being reflective of organisational ambivalence. For example, over the past decade the SIRC has, on a number of occasions, touched on the aforementioned disjoint through their publications. The instance which received the most coverage was the 2006 special commission report entitled, *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.*[30] The

[27] Wesley Wark. "CIPS Policy Brief No. 27 – The Stalemate Over National Security Accountability". University of Ottawa: Centre for International Policy Studies (CIPS), March 2015 http://cips.uottawa.ca/publications/the-stalemate-over-national-security-accountability/

[28] Canada is an anomaly in this respect amongst its allies –it has no security-cleared parliamentary body tasked with intelligence oversight. It's close allies, such as the UK, Australia and New Zealand, each have dedicated parliamentary review bodies with security-cleared members. In: *Ibid.*

[29] Jean Chrétien, Joe Clark, Paul Martin and John Turner. "A close eye on seucirty makes Canadians Safer". *The Globe and Mail*, 19 February 2015. Accessed July 2015 http://www.theglobeandmail.com/globe-debate/a-close-eye-on-security-makes-canadians-safer/article23069152/

[30] Maher Arar is a dual Syrian and Canadian national, who was detained under suspicion of terrorism in the US, and was then deported to Syria (rather than Canada, his place of residence) where he was tortured by the Syrian regime.

SIRC highlighted how the inadequacy of the current system led to one of the most prominent post-9/11 terrorism-related scandals for the Canadian government, and provided recommendations as to how to ameliorate holes in the oversight machinery. However, these recommendations were not heeded, despite the SIRC's instance on the need for improvement. This political ambivalence to needed change, coupled with the introduction of C-51, will only work to further deepen the chasm between expanded powers and stagnated oversight mechanisms.

October 2015, however, will see Canada's next general election. Given the extent to which C-51 – and intelligence oversight, more broadly – has been discussed in the national dialogue amongst civilians and politicians alike, Canadians will have the opportunity to bring this issue to the fore through the ballot box.

| LESSONS FOR A YOUNG DEMOCRACY

Taking into consideration both the effective and ineffective elements of oversight and transparency as they pertain to the Canadian security establishment, this section will provide potential lessons and suggestions that can be adopted by Macedonia.

Ensure that oversight culture is comprehensive

Canada has been criticised for its lack of a broad oversight body responsible for oversight and accountability of the security establishment as whole, with the suggestion that individual oversight bodies responsible to each intelligence service are not enough. Macedonia, similarly, has an ineffective oversight culture especially pertaining to communications intelligence, as evidenced by the recent wiretapping scandal. As such, both should consider the benefits to establishing a comprehensive and complete oversight culture, which encompasses all stages of the intelligence cycle. Completeness in this regard should pertain to a) "the oversight body: the government, parliament, the judiciary, and a specialised (non-parliamentary, independent) commission [...]; b) the moment of oversight: prior oversight, ongoing oversight, and after-the-fact oversight, and; c) the mandate of oversight bodies: reviews of lawfulness and effectiveness".[31]

Foster a culture of political and institutional expertise

A move toward oversight comprehensiveness should be conducted in tandem with fostering a culture of political will and expertise; this is a particularly important element for Macedonia, and is an area in which much can be learned from the Canadian system.[32]

The report in question found him innocent of any links to terrorism and the Canadian government formally apologised for his treatment. In: Security Intelligence Review Committee. *Report of the Events Relating to Maher Arar: Analysis and Recommendations.* Commission of Inquiry into Actions of Canadian Officials in Relation to Maher Arar, 2006.

[31] Sarah Eskens, Ot van Daalen and Nico van Eijk. *Ten Standards for Oversight and Transparency of National Intelligence Services*. (University of Amsterdam: Institute for Information Law, 2015), pp. i.

[32] The Canadian security establishment is quite effective in this regard: for example, the CSE Commissioner must be an individual with judicial expertise, and SIRC members must be individuals with the appropriate security clearance relevant to conducting organisational oversight.

For example, the Macedonian Parliamentary Committee responsible for analysing communication interception has neither the parliamentarians with appropriate qualifications, skills or knowledge for performing effective oversight, nor does it have additional staff members in place to provide research and expertise to the Committee.[33] Additionally, with each election of a new government in Macedonia comes a huge turnover in staff at the country's intelligence agencies, thus leading to a dangerous loss of institutional knowledge.[34] In order to secure effective implementation of oversight mechanisms, it is critical for Macedonia to ensure that its agencies and bodies maintain their institutional expertise by preventing the loss of those with institutional knowledge. Moreover, the parliamentarians which it appoints to its committees responsible for intelligence oversight must be relatively knowledgeable in that field, and be supported by the appropriate staff necessary for comprehensive research and analysis.

Develop oversight measures in tandem with expanding security powers

As mentioned previously, Canada has been criticised for not allowing its oversight mechanisms to grow alongside expanding security powers, thus hindering the effectiveness of those mechanisms. Macedonia, similarly, should not allow itself to fall into a similar predicament. It would be most effective to institute initiatives such as committed review mechanisms; these could take the form of dedicated quadrennial intelligence oversight reviews, similar to the quadrennial defence reviews instituted by the United States.[35] Such an endeavour could help to ensure that oversight mechanisms are meeting the appropriate intelligence needs of the state, especially in light of frequently-changing threatscapes.

Scandal as opportunity for reform

One of the main factors in the significant transparency of CSIS is found in the nature of its creation – it was forged from the fires of its scandal-plagued predecessor, and was created after significant discussion, analysis, and recommendations were put forward in order to create a service which operated more effectively and transparently than its predecessor. As the Macedonian security establishment remains amidst the debris of the wiretapping scandal, it should use this situation as an opportunity for significant and meaningful reform of its oversight mechanisms, and pledge itself anew in a concerted culture of transparency.

Develop and nurture a culture of transparency

In Macedonia, it has been suggested that one of the greatest hindrances to effective oversight is the lack of a culture of transparency.[36] This is coupled with significant distrust from citizens toward their intelligence services, with a staggering 63.6% of citizens believing that the services "intercept the communications to those which are opponents to

[33] Bogdanovski and Lembovska, pp. 34.

[34] This is due predominantly to fact that the security establishment in Macedonia can frequently be the creature of the political party in power. As one member of the Army Intelligence and Counterintelligence Unit stated, "it is considered to be 'normal' for political parties in power to use [an election] and misuse these bodies for their personal political gain". In: Andreja Bogdanovski. Strengthening Intelligence Oversight in the Western Balkans – Macedonia as a Case *Study*. (Skopje: Analytica, 2015), pp. 10.

[35] For example, see: "U.S. Department of Defense – Quadrennial Defense Review". United States Government. Accessed July 2015 http://www.defense.gov/home/features/2014/0314_sdr/qdr.aspx

[36] Bogdanovski and Lembovska, pp. 35.

the current government" and 43% who believe that their privacy has been infringed.[37] The establishment must work to regain the trust of their citizens, lest the toxic relationship become a situation of permanence rather than exceptional circumstance.

Both CSE and CSIS can provide lessons from which the Macedonian security establishment can draw, as both agencies are deeply committed to transparency regarding their mandates, purpose in society, and relationship to Canadian citizens. In light of the wiretapping scandal, it is critical that the Macedonian security establishment re-engage with its citizens in a wholly transparent and open manner; it must create, maintain and foster comprehensive transparency programmes and ethics codes, and implement serious forms of punishment for those in the services who act against their legislative responsibilities. Programmes such as CSIS' "Cross-Cultural Roundtable on Security" could be ideal for an ethnically-diverse country such a Macedonia, as it endeavours to engage citizens in long-term dialogues on defence and security whilst taking into consideration the multi-ethnic composition of Canada. Regardless, whatever new programmes are instituted, it is critical that they be educational, truthful, and transparent; they cannot be platforms for disseminating governmental propaganda.

Natasia Kalajdziovski *is a research intern with Analytica think tank in Skopje. She is a graduate of the Department of War Studies, King's College London, and has single- and co-authored a number of published reports throughout her academic career. Her research interests pertain to morality in intelligence practice, state security responses to domestic terrorism, and home-grown radicalisation. Prior to joining Analytica, Ms Kalajdziovski held researcher positions at the Security Governance Group and the G8 Research Group. In October 2015, she will be commencing PhD study on a fully-funded research studentship at Middlesex University in London.*

[37] *Ibid*, pp. 34.

BIBLIOGRAPHY

Bill C-23. *Canadian Security Intelligence Service Act*. Parliament of Canada, RSC 1985. Amended 23 April 2015 http://laws-lois.justice.gc.ca/PDF/C-23.pdf

Bill N-5. *National Defence Act*. Parliament of Canada, RSC 1985. Amended 1 June 2015 http://laws-lois.justice.gc.ca/PDF/N-5.pdf

Bogdanovski, Andreja. *Strengthening Intelligence Oversight in the Western Balkans – Macedonia as a Case Study*. Skopje: Analytica, April 2012 http://www.analyticamk.org/images/stories/files/report/macedonia_eng1.pdf

Bogdanovski, Andreja and Magdalena Lembovska. *"Making the Impossible Possible": Communications Interception Oversight in Macedonia*. Skopje: Analytica, 2015 http://analyticamk.org/images/Files/impossible_en_final_9af93.pdf

"Canadian Security Intelligence Service – Access to Information and Privacy Section". Government of Canada. Accessed July 2015 https://www.csis.gc.ca/tp/index-en.php

"Canadian Security Intelligence Service – History of CSIS". Government of Canada. Accessed July 2015 https://www.csis.gc.ca/hstrrtfcts/hstr/index-en.php

Chrétien, Jean, Joe Clark, Paul Martin, and John Turner. "A close eye on security makes Canadians safer". *The Globe and Mail*, 19 February 2015. Accessed July 2015 http://www.theglobeandmail.com/globe-debate/a-close-eye-on-security-makes-canadians-safer/article23069152/

"Communications Security Establishment – CSE Ethics Charter". Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/about-apropos/ethics-charter

"Communications Security Establishment – History". Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/history-histoire

"Communications Security Establishment – How is CSE Held Accountable?" Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/inside-interieur/review-examen

"Communications Security Establishment – What We Do and Why We Do It". Government of Canada. Accessed July 2015 https://www.cse-cst.gc.ca/en/inside-interieur/what-nos

"Completed Access to Information Requests". Government of Canada. Accessed July 2015 http://open.canada.ca/en/search/ati

Eskens, Sarah, Ot van Daalen and Nico van Eijk. *Ten Standards for Oversight and Transparency of National Intelligence Services*. University of Amsterdam: Institute for Information Law, 2015 http://www.ivir.nl/publicaties/download/1591

"Public Safety Canada – Connecting with Canadian Communities: Cross-Cultural Roundtable on Security". Government of Canada. Accessed July 2015 http://www.publicsafety.gc.ca/cnt/ntnl-scrt/crss-cltrl-rndtbl/index-eng.aspx

Security Intelligence Review Committee. *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. Commission of Inquiry into Actions of Canadian Officials in Relation to Maher Arar, 2006 http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf

"Security Intelligence Review Committee – Annual Reports". Security Intelligence Review Committee. Accessed July 2015 http://www.sirc-csars.gc.ca/anrran/index-eng.html

"Security Intelligence Review Committee – Looking Back". Security Intelligence Review Committee. Accessed July 2015. http://www.sirc-csars.gc.ca/opbapb/rfcrfx/sc02a-eng.html

"U.S. Department of Defense – Quadrennial Defense Review". United States Government. Accessed July 2015 http://www.defense.gov/home/features/2014/0314_sdr/qdr.aspx

Wark, Wesley. "CIPS Policy Brief No. 27 – The Stalemate over National Security Accountability". University of Ottawa: Centre for International Policy Studies (CIPS), March 2015. Accessed July 2015 http://cips.uottawa.ca/publications/the-stalemate-over-national-security-accountability/

Natasia Kalajdziovski

Oversight and Transparency in the Canadian Intelligence Establishment: **Lessons for a Young Democracy**

Contact
Address: Dame Gruev
No: 7-8/3 1000 Skopje, Macedonia
Tel: 00389 (0)2 3121 948
Fax: 00389 (0)2 3121 948
info@analyticamk.org

www.analyticamk.org