UDK 355.40
https://doi.org/10.18485/fb_ic4hs.2018.9

INTERNATIONAL INTELLIGENCE SHARING: KEY PRECONDITIONS FOR AN EFFECTIVE OVERSIGHT

Luka GLUŠAC*

Abstract: International intelligence sharing has increased in the last twenty years or so, particularly after the terrorist attacks of 11 September 2001. Already established intelligence cooperation agreements, bilateral and multilateral, have entered into a new phase, resulting in a vast amount of intelligence shared, including the information on their own citizens communicated by national agencies both among themselves, and with their foreign counterparts. Some of those intelligence cooperation agreements are formal, constituting legal instruments, but an important number of them are actually informal, based upon the common understanding between heads of the national intelligence services or other state officials. When intelligence exchange is based on informal international cooperation, rooted only in a scarce and usually outdated national legislation, then there are no legal safeguards for the citizens, who are essentially the targets of such an exchange. In other words, these practices have had many human rights implications. While there is a considerable body of literature on intelligence sharing per se, its human rights aspects remain largely neglected. Hence, our aim is to map the preconditions for an effective oversight of international intelligence sharing, concentrating on the external oversight that should be designed to guarantee a legally sound exchange of intelligence with foreign partners.

Keywords: security, oversight, privacy, intelligence sharing, intelligence cooperation

1. INTRODUCTION

Globalisation has created a relatively borderless world in which states move clumsily but wherein their illicit opponents move elegantly (Aldrich, 2008). National governments have placed intelligence in the front line against a range of transnational opponents, coupled with an increased understanding of the importance of international intelligence cooperation. However, at the same time, such a cooperation has been a great challenge, since it is not a natural instinct of intelligence services (ibid). Intelligence services are in

* The author is a PhD Candidate at the University of Belgrade - Faculty of Political Sciences, and Independent Adviser in the Secretariat of the Protector of Citizens (Ombudsman) of the Republic of Serbia, lukaglusac@gmail.com. The views expressed in this article are his own and do not necessarily reflect the positions of the Ombudsman. lukaglusac@gmail.com

constant fear that with intelligence sharing they actually risk not only the disclosure of secret information obtained from secret sources, but a potential exposure of their methods, thus hindering their ability to collect intelligence in the future.

After 9/11, the United States made full use of its foreign intelligence cooperation (liaison) relationships, for both defensive and offensive purposes (Joint Intelligence Committee, 2002). At the same time, inquiries into 9/11 have shown that cooperation between the different services even within one country is often poor (Aldrich, 2010: 21). In the decade since 9/11, many national governments have worked to overcome legal and organisational barriers to information sharing, both on domestic and international levels. The director of Spain's intelligence service publicly confirmed the enhanced level of cooperation among intelligence agencies since 9/11 (Lefebvre, 2003). As a result, the new zeal for information sharing has extended well beyond counterterrorism to a wide array of law enforcement responsibilities including border security, immigration, smuggling, and espionage (Roach, 2012: 131).

There is a considerable body of literature on intelligence sharing, including those on the costs and benefits to each country of engaging in intelligence sharing (see Walsh, 2007; Sims, 2004; Richelson, 1990). When intelligence exchange is based on informal international cooperation, rooted only in a scarce and usually outdated national legislation, then there are no legal safeguards for the citizens, who are essentially the targets of such exchange. However, these human rights aspects of intelligence sharing remain largely neglected in the literature. Hence, our aim is to map the preconditions for an effective oversight of international intelligence sharing that should be designed to guarantee a legally sound exchange of intelligence with foreign partners.

2. WHAT IS INTERNATIONAL INTELLIGENCE SHARING

Intelligence sharing occurs when one state – the sender – communicates intelligence in its possession to another state – the recipient (Walsh, 2007: 154). Some of those intelligence cooperation agreements are formal, constituting legal instruments, but an important number of them have actually been informal, based upon the common understanding between the heads of national intelligence services or other state officials. Such intensified intelligence exchange has not been followed by appropriate legislation, either on national or international level.

Allies routinely exchange intelligence through various bilateral and multilateral means, but the depth and breadth of these exchanges depend very much on their sharing of a common perception of a threat or sets of interests (Taillon, 2002: 174-175). Bilateral cooperation (or so-called liaison) arrangements are a defining characteristic of the intelligence world. Set up formally (i.e. with the signing of a Memorandum of Understanding) or informally (on the basis of an unwritten, gentlemanly agreement), they pay particular attention to the participants' protection of their intelligence (Lefebvre, 2003: 533). They usually cover a wide range of issues, including the sharing of assessments, raw data, or training facilities and the conduct of joint operations, some of which could lay dormant at any given time (ibid: 533).

Multilateral intelligence sharing arrangements also cover an array of potential activity between governments including, *inter alia*, information sharing, operational cooperation, facilities and equipment hosting, training and capacity building, and technical and financial support. One of the most known arrangements is the Five Eyes alliance – a secretive, global surveillance arrangement comprised of the relevant intelligence agencies of United States, United Kingdom, Canada, Australia and New Zealand, recently referred to as "the most comprehensive and closest intelligence sharing and co-operation arrangement" (Cullen & Reddy, 2016: 46). Although it is a long-lasting alliance with over 70 years of history, little is known about it and about the agreement(s) that governs it. Even less is known about the other surveillance partnerships that have grown from the Five Eyes, such as the 9-Eyes, the 14-Eyes, and the 43-Eyes (see: Privacy International, 2017).[1]

3. HUMAN RIGHTS ASPECTS OF INTERNATIONAL INTELLIGENCE SHARING

Although there is a wide agreement that international intelligence sharing is necessary for countering contemporary threats, its recent expansion has raised a number of potential problems that require vigilant oversight. Individuals are at greater risk of having their rights, especially their right to privacy, infringed. As noted by Roach, individuals will rarely have the opportunity to challenge the accuracy of shared information because they will often be unaware that information about them has been shared and will not have access to the shared information (Roach 2012: 131).

Probably the most obvious human right at risk in this case is the right not to be subject to torture or other forms of cruel, inhuman, or degrading treatment. For instance, information sent to a foreign agency may be used by that agency in support of extrajudicial detention, torture, and even killings. Conversely, information received from a foreign agency may have been obtained through torture or be otherwise tainted (Roach, 2012: 134). Thus, a special care should be taken when sending questions to foreign agencies, not only because they may invite the use of harsh interrogation tactics, but also because foreign agencies may use such questions in a way that is even less amenable to control by caveat (Arar Commission, 2006). In principle, information should never be provided to a foreign country where there is a credible risk that it will cause or contribute to the use of torture (ibid: 345). The UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism recommended that "before handing over information, intelligence services [should] make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and, will not be used for purposes that violate human rights" (UN Human Rights Council, 2010: 46). While this recommendation may seem idealistic, it indeed grasps the very *credo* of human rights-sensitive international intelligence sharing.

[1] For other multilateral intelligence agreements see, for instance: Lefebvre, 2003.

4. MAPPING THE PRECONDITIONS FOR AN EFFECTIVE OVERSIGHT

The sharing of information with foreign agencies generally presents the greatest challenge to oversight bodies and one of the permanent risks to human rights. It is, thus, vitally important that oversight bodies have access to the information being shared by the agencies they oversee — whether or not that information is subject to the claims of secrecy. The above-mentioned UN Special Rapporteur stated that "it is good practice for national law to explicitly require intelligence services to report intelligence-sharing to an independent oversight institution" (UN Human Rights Council, 2010: 49). To facilitate that, intelligence sharing should, preferably, be developed through written agreements, specifying the obligations of both sending and receiving parties with regard to human rights. They should also include standard clauses that permit received information to be shared with the service's principal oversight body and, when possible, with related oversight bodies that agree to the same confidentiality protocols. In other words, intelligence sharing with foreign partners should always be well documented because of the risks involved, and also facilitate review and oversight (Roach, 2012: 137).

While every state chooses its own institutional setup for the oversight, it is widely acknowledged that there has to be a complex oversight system, designed through various forms: internal and external; political and expert; judicial and quasi-judicial; *ex ante* and *ex post* (Glušac, 2018). Given that the oversight powers of particular institutions differ in nature, scope and reach, a high level of cooperation and coordination between them is necessary, both in normative and operational terms (ibid: 19). For instance, in some countries, such as Germany and Serbia, competent parliamentary oversight committees are not granted access to shared information because they are considered to be the so-called third parties.[2] However, in case of Serbia, shared information can be accessed by the Ombudsman, as an independent oversight mechanism.[3]

A totality of individual mandates of oversight bodies should ensure that such oversight system is able to scrutinize at least the following aspects of international intelligence cooperation: (1) effectiveness of cooperation with foreign entities; (2) the legal and (operational) policy framework for international intelligence cooperation; (3) high-risk relationships; (4) risk assessment processes; (5) personal data exchanges and their human rights implications; (6) caveats and assurances relating to information sent to foreign services; (7) reporting and records keeping; (8) joint operations; (9) provision of training and equipment to foreign services; (10) services' training of their own staff; (11) financial transactions relating to international intelligence cooperation; and (12) the role of the executive in international intelligence cooperation (Born, Leigh, & Wills, 2015: 134-143).

Scholars have identified different methods used by overseers to scrutinize international intelligence cooperation, including hearings, documentary analysis, interviews, sampling, and direct access to databases (ibid: 143-150). External overseers may use different types of investigations, such as case-specific, thematic, comprehensive and/or periodic.

---

[2] More on third parties in: Born, Leigh, & Wills, 2015: 152-154.

[3] For more on the Ombudsman's role in oversight of the security services see: Glušac, 2018.

Oversight bodies should understand that intelligence services sometimes use intelligence sharing as a means of avoiding national (domestic) restrictions on their activities. Hence, intelligence services should be "explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities" (UN Human Rights Council, 2010: 49-50).

5. CONCLUSION

To sum up, in order to create an effective oversight system of international intelligence sharing, some basic principles have to be followed. Intelligence services need to be subject to oversight that is complete, i.e. it should encompass all stages of the intelligence cycle. Oversight should be both *ex ante* and *ex post*, but also internal and external. External elements of the oversight should include judicial and expert specialised bodies. Such bodies should be independent, and able to provide for redress. Redress should be provided through, *inter alia*, own-initiative investigations and individual complaint-handling procedures, when applicable. Ombudsman or similar specialised (external) body can act as quasi-judicial mechanism, complementing the work of judiciary. Irrespective of the institutional design, such mechanism should have broad mandate and sufficient resources to perform effective oversight. Those bodies should also serve to provide layered transparency, which is of critical importance in a democratic society.

As argued in this paper, international intelligence sharing should be regulated by written agreements, whenever possible. It is expected that, in most circumstance, making such an agreement in writing would not have negative consequences on its implementation, but would enable oversight that is more robust.

Finally, as national intelligence agencies share information in order to be able to fulfil their mandates, national oversight bodies should do the same. A step in the right direction is a recent initiative of independent oversight bodies in five countries which agreed to establish the Five Eyes Intelligence Oversight and Review Council "to facilitate the sharing of experiences and best practice in oversight and review" (Australian Inspector-General of Intelligence and Security, 2017: v).

6. BIBLIOGRAPHY

Aldrich, R. J. (2008). Setting Priorities in a World of Changing Threats. In S. Tsang, *Intelligence and Human Rights in the Era of Global Terrorism* (pp. 158-171). Stanford: Stanford University Press.

Aldrich, R. J. (2010). International Intelligence Cooperation in Practice. In H. Born, I. Leigh, & A. Wills, *International Intelligence Cooperation and Accountability* (pp. 18-41). New York: Routledge.

Australian Inspector-General of Intelligence and Security. (2017). *Annual Report 2016-17.* Barton: IGIS.

Born, H., Leigh, I., & Wills, A. (2015). *Making International Intelligence Cooperation Accountable.* Geneva: DCAF.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. (2006). *Report of the Events Relating to Maher Arar: Analysis and Recommendations.* Ottawa: Privy Council.

Cullen, M., & Reddy, D. P. (2016). *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand.*

Eskens, S., van Daalen, O., & van Eijk, N. (2015). *Ten Standards for Oversight and Transparency of National Intelligence Services.* Amsterdam: University of Amsterdam - Institute for Information Law.

Glušac, L. (2018). National Human Rights Institutions and Oversight of the Security Services. *Journal of Human Rights Practice, 10*(1), 58–82.

Joint Intelligence Committee of the US Senate and US House of Representatives. (2002). *Investigating the Events Leading to the Attacks of September 11, 2001*. Washington, DC.

Lefebvre, S. (2003). The Difficulties and Dilemmas of International. *International Journal of Intelligence and, 16*(4), 527-542.

Privacy International. (2017). *Human Rights Implications of Intelligence Sharing.* London: Privacy International.

Richelson, J. (1990). The Calculus of Intelligence Cooperation. *International Journal of Intelligence and Counterintelligence, 4*(3), 307-323.

Roach, K. (2012). Overseeing Information Sharing. In H. Born, & A. Wills, *Overseeing Intelligence Services: A Toolkit* (pp. 129-150). Geneva: DCAF.

Sims, J. (2004). Foreign Intelligence Liaison: Devils, Deals, and Details. *International Journal of Intelligence and CounterIntelligence, 19*(2), 195-217.

Taillon, P. (2002). Hijacking and Hostages: Government Responses to Terrorism. Westport: Praeger.

UN Human Rights Council. (2010). Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Walsh, J. I. (2007). Defection and Hierarchy in International Intelligence Sharing. Journal of Public Policy, 27(2), 151-181.