DCAF Geneva Centre for Security Sector Governance

Expert Opinion

on the draft laws on

The Security and Intelligence Service of the Republic of Moldova (SIS law)

The counterintelligence activity and the external intelligence activity (CI law)

DCAF Project

Strengthening Security Sector Governance in Moldova

SSGM

Supported by Sweden

Sweden Sverige

Background and methodology

DCAF was requested[1] to provide an expert opinion on the **Draft Laws on the Security and Intelligence Service of the Republic of Moldova (SIS law) and the counterintelligence activity and the external intelligence activity (CI law).**

This expert opinion is based on the conclusions and recommendation made by **four senior intelligence experts** engaged by DCAF in the review process. The senior experts have extensive knowledge and experience in intelligence reform and governance, having worked in management roles in intelligence services in EU member states (Austria, Poland, Slovenia, and UK). Therefore, they have first-hand experience of the challenges faced by European intelligence services in organising effective and efficient intelligence processes that enable adequate responses to security threats and are subject to functional control and oversight mechanisms. In addition to their careers within their respective national security sectors, the senior experts have provided technical advice to various parliaments and intelligence services undergoing reform processes in post-soviet countries,

Each of the experts individually analysed the two draft laws and have submitted their **separate findings** to DCAF. Their analysis of the draft laws was conducted between mid-February and mid-March 2023. Consequently, their assessments did not take the findings of the Venice Commission Opinion, published on 14 March 2023, into consideration. The four reviews have been analysed and **integrated into one common opinion**, written by the DCAF "Strengthening Security Sector Governance in Moldova" project team.

From the technical standpoint, the experts provided general opinions, but did not apply the traditional method of benchmarking the draft law article by article against similar laws implemented in other countries as **the drafts are not similar with existing legislation in EU** member states. In order to keep this text to a limited number of pages, the assessment of provisions that are sufficient and clear have been omitted from this review. Rather, this this review highlights the **major concerns** and **potential shortcomings** of the two drafts.

Summary of findings

Despite conducting the assessment of the laws independently from each other, and from the Venice Commission, the **conclusions of the four DCAF experts are very similar** and endorse **the main findings of the Venice Commission Opinion**. Below is a summary of main findings:

[1] Through a letter signed by the chairman of the Committee for national security, defence, and public order, signed on 30 January 2023

Overall assessment

1. The two draft laws **require <u>further careful consideration</u> and <u>thorough amendment</u>** in order to deliver the legal foundation of a security and intelligence service that is (1) <u>effective in deterring threats to national security</u> and (2) <u>democratically accountable</u> in the fulfilment of its mission.

2. The two draft laws are complex and **over-ambitious on defining SIS powers and operational responsibilities but provide little detail and few clear provisions on control and oversight.**

On wording and structure (law making procedure)

3. It is extremely important to harmonize the draft laws with the **National Security Strategy** (NSS) and the definition of "**national security**", "**threats to national security**", and "**national interest**" defined by the NSS. Ideally, the debate and the approval of NSS should precede the debate of statutory laws for SIS.

4. Both draft laws over-detailed and complicated, yet vague on some of the more important issues. Similar laws in European democracies are simple (rarely over 6 pages), less detailed on operational activity, and define the important issue of oversight in all its forms (executive, parliamentary, and judicial) in greater detail.

5. The decision to draft **2 separate laws** (also a third law on the role of the intelligence officer) should be further considered, along with the possibility of combining the drafts into a single law. A single law would avoid repetitions, provide greater clarity, and be a single point of reference for intelligence activity. If two laws are kept, clarity and harmonization must be ensured, especially on tasks and powers of the service.

6. The word choice in Chapter II of the SIS law is questionable, as it talks about the "rights" of the service. An intelligence service has "obligations", "responsibilities", "powers", and "authorities". "Rights" - a set of legal entitlements or protections that are granted to individuals to ensure their safety, security, and well-being - generally pertain to individuals rather than to state authorities. The use of the concept "rights" in association with the intelligence service might go against the spirit of democratic legislation oriented towards human security.

On the functionality and effectiveness of SIS

7. **Powers and Tasks**. SIS powers and responsibilities are very broad (Art. 5, 6, 8, 13 of SIS law); such a wide mandate goes far beyond the intelligence service models in EU/NATO countries. Moreover, the list is inconsistent, as typical intelligence tasks are mixed up with powers and means of carrying out tasks. The **main risk** of assigning such an extensive and diverse range of powers to a service is **inefficiency** – through the fragmentation of its efforts and incoherent, confusing tasking.

8. Executing **an extensive range of tasks would require an institutional capacity that is difficult to ensure**: extensive, highly skilled human resources and a large budget. In Budget Law, SIS has an allocation of about 20 million euros. It seems therefore that the large mandate envisaged by the law is disproportionate to the existing capabilities of SIS.

9. Performing such complex, numerous, and varied tasks will be a difficult, if not impossible, endeavour in practice. The tasks will require a wide range of staff profiles and professional experience. The **recruitment, training, and retention of staff** for these tasks will be a challenge.

10. By explicitly and comprehensively defining all possible activities of SIS, **the laws do not allow for flexibility in operations** (especially during a time of national emergency). The long, all-encompassing list of tasks and powers provided for in the SIS law may result in the service hiding behind the law rather than taking responsibility for its actions and explaining whether the work they are doing is for the good of society in general.

11. This extensive mandate also creates **overlap between SIS and a number of other state institutions**, including the armed forces, law enforcement, and diplomacy. This risks burdening the SIS with tasks and responsibilities for matters they will not be able to implement because those tasks and responsibilities are the statutory responsibility of other state authorities. Whilst it is important that SIS have an advisory role, executive responsibility for some of the tasks enumerated by the SIS law would ideally be delegated to other authorities.

12. Equipping one sole service with such extensive powers, without strong and effective oversight and control mechanisms, inevitably leads to **inefficiency and abuse of power**. The kind of intelligence service envisaged by the draft law suggests an omnipotent service in an authoritarian regime, not a functional service well-integrated into a democratic system. The practice of the EU/NATO intelligence services proves that effectiveness relies on a well-informed division of coherent, clearly defined, and limited amount of tasks between several services, each of which focuses on a separate, precise goal (mission).

13. For intelligence activities to be conducted effectively, the service and its personnel should be relieved from additional tasks that are unrelated to the collection of information. SIS would probably benefit from having less responsibilities in order to **concentrate on counter-intelligence** work at a time of national emergency. Examples of powers/responsibilities that could be reduced:
    - In most democratic societies, intelligence services are not granted **police powers**. This is because intelligence activities - both foreign and internal (including counterintelligence) - are focused on collecting, analysing, and distributing intelligence relevant for national security decisions to the executive authority. Criminal prosecution of crimes is an activity serving other purposes, i.e. obtaining evidence for use in court, and usually it is not the task of the intelligence services. Intelligence officers are not typically trained or equipped to engage in law enforcement activities. In addition, the essence of the activities of intelligence

services is secrecy which requires very strong restrictions on access to the information they collect and intelligence they produce. This, in turn, requires the circle of recipients of intelligence materials and entities authorized to commission them with tasks to be limited. The proposed list of such entities is far too broad and diverges from EU/NATO practices and standards.

- The protection of national critical infrastructure mentioned in Art. 7 (f) is a task often assigned to law enforcement.
- The protection of diplomatic premises and the obligation to ensure diplomatic courier services would absorb limited human resources and distract the service from key tasks. It may even give rise to conflicts, e.g. with the Ministry of Foreign Affairs. This task could be delegated to other agencies. The SIS should retain only its advisory role.
- The authority on state secrets (National Security Authority) is usually assigned to an independent civilian institution.

14. External work. Chapter III of the CI law should further consider the implications of external operations, their legality, and the implications for individual officers. The draft does not take SIS officers committing illegal acts (such as bribery) when operating overseas into account . This would render SIS officers subject to prosecution not only in foreign countries but also in Moldova if Moldovan law is extraterritorial i.e. the act is liable for prosecution for a Moldovan citizen in Moldova even if carried out overseas. Other similar services avoid this through specific parts of their legislation. For example, in the UK this is covered by section 7 of the ISA in which ministerial approval is needed for officers to break the law overseas but provides effective immunity from prosecution in the UK. In the US, this falls under the various presidential decrees.

15. The draft laws are silent on many aspects that involve (criminal) liability of officers. Some examples are cases of influencing, supporting, or adopting decisions contrary to national interest and illegal orders, degradation, or destruction of economic resources of national interest. It is also unclear if officers or collaborators can participate or contribute to crimes or act as *agent provocateur*. The obligation on crime reporting is too narrow – even petty crime must be reported.

On the Security Mandate

16. The essence of intelligence activity is the **collection of intelligence information** useful in the decision-making process of state authorities. The aim is to gain reliable, prescient knowledge **about threats and risks to national security** in order to prevent and neutralize them. The effectiveness of intelligence activity is determined by the accuracy, reliability, and punctuality of the intelligence provided to decision makers and **not** by the evidentiary value of the information collected.

17. The information collected through covert methods such as secret surveillance or interception of communications that infringe human rights and liberties, especially the right to privacy, aims at providing insight that allows the intelligence service to prevent and deter threats to national

security. In most European countries, intelligence services use such intrusive methods for information collection under the following circumstances:

- A mandate/warrant is authorised by an authority external to the service;
- The mandate is issued **outside the framework of the criminal process** because it often concerns issues that are not subject to criminal assessment; therefore, the authorisation process is regulated by other laws than Criminal Procedure Code (the statutory law of the intelligence service or a special law on special investigative measures);
- The request for using such measures may be triggered by **lower standards/grounds of suspicion** than the use of intrusive measures in criminal investigations, the purpose of which is to collect evidence of crimes that have already been committed;
- The request is subject to **different mechanisms for control and oversight** from those concerning law enforcement agencies: the approval of the service Director for each request is followed by a judicial warrant issued by a high-level court or a specialized court; a special oversight parliamentary committee or independent oversight body exercise post-facto oversight over the legality, legitimacy, and proportionality of such measures;
- In most European countries the prosecutor does not play a role in the approval of the security mandate;
- The principles defined by the jurisprudence of the European Court of Human Rights (such as **legality, necessity, legitimacy, proportionality, subsidiarity,** or ultima ratio) should be of binding nature for authorities involved in the initiation, authorization, and implementation of intrusive methods – intelligence officers, intelligence service director, court.

18. One of the fundamental conditions for the effectiveness of intelligence services is the **secrecy** of both persons and structures engaged in intelligence activities, as well as methods, forms, and means of conducted activities. While law enforcement activities are conducted with much less secrecy and often in conditions of openness, maintaining intelligence secrecy gives rise to a number of requirements related to the organization of the activities of such a service, both in the country and abroad. This is another reason for which the involvement of service staff and infrastructure in non-intelligence tasks should be avoided.

On the accountability system of SIS

19. Effective safeguards should be created to prevent intelligence services from engaging in activities and collecting information for purposes other than preventing threats to national security. An effective accountability system aims mainly to prevent (1) the misuse of state funds and (2) abuse of powers (such as interference in the political situation, restriction of civil liberties, persecution of citizens, illegal and/or unjustified use of intrusive measures for information collection, and manipulation of the information obtained for purposes contrary to the tasks of the service, including conducting criminal activities by the officers of the service).

20. Different levels of control and oversight contribute to intelligence accountability. They are complementary and mutually reinforcing, so deficiencies in one level have the potential to affect the entire system.

Internal control

21. Internal control systems translate abstract legal provisions into administrative and 'day-to-day' operational instructions and serve the purpose of identifying and neutralizing cases of abuse of powers and other irregularities by service personnel. The functionality and efficiency of the internal control system should be subject to assessment by external control bodies. Together with senior members of the SIS, government and parliament should consider what internal controls should be put in place to ensure the working culture and methodologies reflect the democratic and societal norms of Moldovan society. Internal controls and culture are as important as legislation.

22. Internal control mechanisms within the SIS are not sufficiently detailed in the two drafts. The responsibility for ensuring internal control is given to the SIS Director (SIS Law art.18 i) and CI law art. 59) in the laws in a laconic and general way. However, both laws are silent on the establishment and functioning of internal control mechanisms. The draft laws make no mention of how the Director should fulfil this responsibility and how the internal control system will be overseen by the executive and legislative branches. The laws should specifically give the Director the responsibility to establish ethical guidelines within the service that reflect the values of Moldovan society.

23. The law should be supplemented with **clear provisions defining the goal, scope, mechanisms, and rules** of the internal control system, as well as forms and means for achieving the goal. Internal control should be a system that is integrated into the service at all levels of management. The activities of the internal control sub-units (Art.59(1)) are only a part of the so-called internal institutional control. Part of the internal control system is also operational control instruments such as the Director`s decisions to authorise counter-intelligence measures (Article 14) and external intelligence activity (Article 49).

24. Clear and strong internal control mechanisms are an essential prerequisite of a culture of self-restraint in the use of intrusive methods. Therefore, much attention should be given to the development of bylaws, regulations, professional standards, codes of conduct, and personnel training, following the adoption of the legislative package.

25. The provision regarding the destruction of materials that have proven to be irrelevant to the investigated case is confusing and contrary to the principles of internal control (Art 10 and 56(2) of CI law).

Executive control

26. Executive control is unclear – especially the tasking of SIS. Intelligence tasking is the process of setting key intelligence requirements and priorities that define intelligence agency spending and the collection and analysis of intelligence. In democracies, intelligence tasking is the responsibility of the executive branch of government and reflects a state's foreign, security, and defence policies. The output of the tasking process, commonly referred to as a 'statement of intelligence priorities', is usually summarized in a document that is approved by government ministers or the head of the executive. Parliaments do not directly task intelligence agencies as it is the executive who controls the policies, strategic planning, and actions of the public sector.

27. Both draft laws lack detail (if any definition at all) on how the SIS is tasked. When organizing intelligence activities, it is necessary to consider the creation of an effective and efficient system of tasking of intelligence services by precisely designated executive authorities. This is instrumental for ensuring that the SIS is carrying out priorities as defined by the government and that their activities comply with national interest and the real needs of state authorities. In addition, clear tasking is essential for holding the SIS accountable to a clear set of objectives, thus enabling meaningful oversight by the parliamentary committee.

28. The tasking falls to the executive power, ideally to the cabinet rather than the President to avoid tasking that is solely beneficial to the President. In many countries tasking falls to the National Security Council, consisting of the President, senior ministers, and senior defence and security officials.

29. Executive control should be more transparent and clear, in terms of lines of responsibility, and open to oversight in a general way.

Judicial control

30. Judicial control consists in the **ante-facto/ex-ante authorisation** of the use of intrusive methods for information collection (issuing of a warrant), and the **post-facto/ex-post review** (ongoing monitoring) of the application of the warrant. In most European countries, a high-level court (Supreme Court or Appellate Court), through its leadership (President of the Court or a judge assigned by the President), has the legal right to authorise the use of intrusive methods by intelligence services. The high level of the court and the seniority of the judge(s) who have the authority to issue a warrant is meant to **prevent any undue influence** of the intelligence service over their decisions.

31. The SIS draft law does not provide for judicial control mechanisms. The CI law provides detail on the role of the judiciary and the issuing of warrants. The solution envisaged by the draft law **diverges from European good practice in two ways**: (1) the judge issuing the warrant is an instruction judge, not a senior judge from a high-level court; (2) a significant number of intrusive

measures (11 out of 20 defined by the CI law) escape judicial control, being approved by the SIS Director (Art.12 (1) 1).

32. It is unclear how the implementation of warrants is monitored/reviewed by the court, as Art.18 seems to refer only to the information of the SIS Director about the results of a counterintelligence measure. More detail could be provided on the extension of the warrant, specifically the type of information to be provided to the judge and the criteria for granting an extension of the warrant (Art.17 (5)).

33. It should be clear that the judge, when his/her permission is sought for surveillance, does not simply decide a yes/no issue but has full control (within the law) over the *extent* of the permitted surveillance. In other words, the judge can, and should, be able to vary the order, set additional conditions for surveillance, limit the circle of suspects who can be subjected to surveillance, and require the applicant to report back frequently on the results of the surveillance. The law must foster an informed, independent, and critical scrutiny of applications by the judge.

34. In most European countries, the prosecutor does not play a role in authorizing the use of intrusive methods by intelligence services, but has a role in investigating criminal offenses perpetrated by intelligence officers. The provision of Art. 32 on the control of the public prosecutor general is vague and does not specify the scope or form of control. The CI draft law in Art. 58 is more detailed on public prosecutor control, but still vague, leaving many questions unanswered. For example, paragraph 1 indicates that it concerns counterintelligence activity, leaving aside external intelligence activities. Paragraph 2 restricts the scope of the prosecutor role to dealing with complaints against the SIS in cases which may involve a breach of law by service officers. This is a significant narrowing of the scope of prosecutorial control. In addition, the draft law does not address issues such as the tools, procedures, and means on the basis of which prosecutorial proceedings are to be conducted. There are also no indications as to the procedure for handling the results of such proceedings.

35. The legislation would be improved by making the articles simpler and by covering all judicial responsibility in one section. This also illustrates how having one single law instead of two would appear beneficial, in terms of law clarity, brevity, and foreseeability.

Parliamentary oversight

36. Parliaments are the primary body charged with exercising oversight of the implementation of national security priorities by intelligence agencies. As it currently stands, the texts of the draft laws touch on the issue briefly and superficially**. Law provisions should undergo further expansion and better define parliamentary oversight tools.** While the debate triggered by the annual activity report of the SIS is well presented in Art. 57 of CI draft, this is just one tool and one instance for which the oversight power of parliament is exercised. Other tools, such as committee hearings, specific reports requested by the committee, budget approval and budget

execution oversight, field inspections, and questions and interpretations in the plenary, should be mentioned in the law to prevent a minimalistic interpretation of the law's provisions and of the parliament's constitutional power for oversight.

37. Effective oversight relies on the actual authority of a parliamentary committee to summon officials to committee meetings and request **access to information**, documentation, and explanation about the service's activities. This means the members of the committee have access to classified information and the law provides for **sanctions** (that can include criminal liability) for obstructing the committee's access to information or providing the committee untruthful information. MPs` access to classified information pertaining to the SIS should be mentioned by the law.

38. For effective intelligence oversight, the oversight **mandate must be clear and precise** (detailed in a document such as Committee Rules of Procedure) as the access to classified information is always conditioned by the "**need to know**" principle, which at its turn is defined by committee mandate. If parliament does not clearly define its oversight mandate (therefore its "need to know"), this will be informally defined by the SIS which will be inherently restrictive. The law could mention that the committee/subcommittee will define its oversight mandate and modus operandi in a **committee Rules of Procedure**.

39. The law should also provide for an **annual report to be prepared by the committee** or subcommittee and presented to the Parliament in the plenary, reviewing the oversight activities of the committee and their main conclusions and recommendations referring to SIS activity (without referring to sensitive or classified information). Two versions of this report could be envisaged: one restricted(for the Bureau of the Parliament only) and one public (for the plenary and the public).

40. The experience of European countries has shown that it is always best for security and intelligence services to have a **separate, standing parliamentary committee** for oversight rather than a sub-committee. Credible and effective oversight depends on the committee`s solid democratic legitimacy and feasible quorum. The Moldovan Defence Committee should retain the general responsibility for intelligence oversight, consider adopting procedures that increase the functionality of the SIS subcommittee, and encourage it to perform as a tool for channelling opposition views and initiatives. An eventual division of tasks/tools, and opportunities for oversight, between the committee and the sub-committee should be considered.

41. While parliaments are not directly involved in the tasking of intelligence agencies, they nevertheless play a crucial role in overseeing the process. This role is twofold: overseeing the process through which the executive defines intelligence priorities; and, secondly, overseeing the execution by intelligence agencies of these priorities. The committee should carefully consider parliament's direct involvement in tasking intelligence agencies as it might undermine the ability of the executive to govern. Furthermore, this could create a conflict of interest:

parliaments may not carry out independent and effective oversight or scrutiny of intelligence agencies while at the same time being responsible for their tasking.

Other issues related to human rights and fundamental freedoms

42. The question of **interception** of all personal communications is always a difficult subject and needs clear direction and oversight. This is particularly important given that so much of an individual's personal information is carried in data. The CI law is slightly confusing and would benefit from a separate section dedicated to interception protocols which would include storage, deletion of non-relevant material, time limits, deletion of operational material and privileged material i.e. medical, lawyer/client etc., and other matters relating to privacy. In most democratic countries there are separate and specific laws relating to this subject so that all agencies who need to carry out interception follow the same rules.

43. There should be a **limitation to the types of persons/entities who can collaborate** with the SIS. In western countries, certain professions like lawyers, priests, psychiatrists, and journalists, are obliged and have the right to secrecy. In both draft legislations these professions are not mentioned.

44. Data protection provisions throughout the two drafts might not meet European standards.

45. Complaints. There does not appear to be a formal complaints procedure for dealing with complaints against the SIS from the public. The responsibility for investigating complaints lies with the Prosecutor General's office but seems to be restricted to the use of intrusive methods (art.58 of the CI law). However, the public complaints system should be more transparent, clear, and accessible and should include reference to measures and lines of responsibility for correcting irregularities uncovered by the investigation of complaints.

46. The amendment to the Law on the status of the security and intelligence officer awards intelligence officers with new facilities and special powers. For example, entry into restricted access spaces. Even if such a right can be contained in the security mandate, it must be balanced with public interest and respect for human rights.

47. Informing the person about CI measures carried out against them (Article 23). A number of democratic countries carry out this practice, however, this procedure should be considered carefully, as it might alert individuals on methods used by the SIS thus rendering them difficult to use in future. It also has the serious implication of alerting foreign players to SIS's interests and might also affect the ability of the SIS to work with international partners who might be cautious about eventual exposure of shared information and techniques.

Recommendations

- A single, simpler law on the responsibilities of the SIS and its officers might be a better solution. The law would define responsibilities, activities (but broadly), oversight, and tasking.
- A separate law relating to the interception of communications that covers all agencies involved in this work would be beneficial and would remove the perception that the SIS has a privileged role in interception.
- The remit and responsibilities of the SIS are very broad. The SIS would benefit from having less responsibilities in order to concentrate on national security. The formation of joint working teams in other ministries would be one way of resolving this.
- Overlapping competencies with law enforcement bodies, such as the police force, criminal investigation bodies, or anti-corruption bodies, should be avoided.
- The sections on oversight should include more detail. The possibility of a separate parliamentary committee to carry out oversight should be considered.
- The tasking process should be made more transparent and open to oversight in a general way. The oversight of detailed operational matters could compromise national security but the mechanisms of tasking should be open to oversight.
- The implications of external operations, their legality, and the implications for individual officers should be further considered.
- Along with senior members of the SIS, the government should consider internal controls to put in place to ensure that the SIS's working culture and methodologies reflect the democratic and societal norms of Moldovan society. The responsibility for ensuring this could be enshrined in the law to the SIS Director.
- The legislator should keep in mind that much of the basis of the ethical and democratic activity of intelligence services is defined by internal controls and the culture of the service which is difficult to define in legislation. Therefore, after the enactment, the legislator should oversee cautiously how laws are implemented, including through the adoption of internal regulations and professional codes of ethics.
- The SIS law must include explicit regulations regarding good governance principles, accountability, efficiency, and effectiveness.