



# **Enhancing the Intelligence and Security Sector Reforms in North Macedonia through Active System Analysis and Multi-Stakeholder Reflections**

**Roadmap with Performance  
Indicators for Assessing  
Transparency, Accountability,  
and Effectiveness in the  
Intelligence and Security  
Sector of North Macedonia**

This Roadmap is part of the intervention “*Enhancing the Intelligence and Security Sector Reforms in North Macedonia through Active System Analysis and Multi-Stakeholder Reflections*” produced within DCAF-implemented **Intelligence and Security Sector Reform Programme in the Republic of North Macedonia (2021-2026)**. This Roadmap reflects and summarizes the findings - practical and instrumental – based on evidence and qualitative primary data retrieved from interviews, open-ended questionnaires and nominal-group discussions with representatives from intelligence and security sector and independent actors.

The views expressed in this Roadmap are those of the C3I and do not reflect the views of DCAF, the donors or the institutions referred to or represented within this publication.



#### Authors:

Metodi Hadji-Janev (author)  
Ljubica Pendaroska Krstevska (contributing author)  
Dimitar Bogatinov (contributing author)

#### Editor:

Marija Jankuloska

© DCAF, 2024. All rights reserved.

Skopje, 2024

#### About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

DCAF - Geneva Centre for Security Sector Governance  
Maison de la Paix  
Chemin Eugène-Rigot 2E  
CH-1202 Geneva, Switzerland  
Tel: +41 22 730 94 00  
info@dcaf.ch  
www.dcaf.ch  
Twitter @DCAF\_Geneva

CIP - Каталогизација во публикација  
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

351.74.07(497.7)(047.31)  
355-3.07(497.7)(047.31)  
355.40.07(497.7)(047.31)

HADJI-Janev, Metodi

Enhancing the intelligence and security sector reforms in North Macedonia through active system analysis and multi-stakeholder reflections  
[Електронски извор] : roadmap with performance indicators for assessing transparency, accountability, and effectiveness in the Intelligence and Security Sector of North Macedonia / [authors Metodi Hadji-Janev (author) ; Ljubica Pendaroska (contributing author), Dimitar Bogatinov (contributing author)]. - Skopje : DCAF – Geneva Centre for Security Sector Governance, 2024

Начин на пристапување (URL):

<https://c3initiative.com/mk/category/aktivnosti/>. - Текст во ПДФ формат,  
11 стр., илустр. - Наслов преземен од екранот. - Опис на изворот на ден  
17.09.2024

ISBN 978-608-5046-01-0

1. Pendaroska Krstevska, Ljubica [автор] 2. Bogatinov, Dimitar [автор]

а) Безбедносен сектор -- Добро управување -- Патоказ на индикатори -- Македонија -- Истражувања

COBISS.MK-ID 64434949

# DEFINITIONS

**Transparency** in the security sector presupposes the publicity, accessibility, and visibility of actions, measures, costs and effects of some activity. It is critical for ensuring good governance of the intelligence and security sector and represents openness to public scrutiny by providing opportunities for access to information, regulations, activities, and processes.

**Accountability** necessitates the existence of mechanisms that ensure the security sector is held responsible for its actions, decisions, and undertakings in fulfilling its duties. Accountability can take the form of soft (informal) and hard (formal) accountability and can be either horizontal or vertical. The presumptions for effective accountability of security sector typically relies on a strong civil society, consolidated institutions, and legislative underpinning.

The ‘transparency and accountability’ principles are crucial in preventing the misuse of the security sector for political purposes, as well as hindering corruption practices. These principles are essential in securing public trust and legitimacy of security institutions.

**Efficiency** and **effectiveness** are two intertwined principles that refer to the overall quality of the results of the security provision. Effectiveness refers to the extent to which intelligence and security institutions fulfill their roles and responsibilities to the highest standards. Efficiency, on the other hand, implies fulfilling these roles and responsibilities with the optimal utilization of public resources.<sup>1</sup>

The **digitalization of the security sector** is a process of impacting the way/manner the work of the security sector is optimized using digital tools. The development of information and communication technologies (ICT) opens new opportunities for improvement of the performance, optimization of human capital and resources, better supervision and control, and greater inclusion of the independent actors in the reform,

## UPHOLDING DIGITALIZATION OF THE MACEDONIAN INTELLIGENCE & SECURITY SECTOR IN BROADER SENSE, AMONG OTHERS, WILL:

- enhance overall functionality,
- improve the ability of the sector to strategically communicate,
- optimize leadership and management processes within the sector,
- improve cross sectorial communication as an imperative of holistic solutions under the contested security environment,
- improve transparency and accountability,
- enhance the legislative procedures,
- improve efficiency and reduce time and cost,
- improve the return on investment,
- increase inclusiveness and trust.

<sup>1</sup> DCAF, SSR BACKGROUNDER, Security Sector Governance, available at [https://www.dcaf.ch/sites/default/files/publications/documents/DCAF\\_BG\\_1\\_Security\\_Sector\\_Governance\\_EN.pdf](https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf)

monitoring and oversight processes. Digital transformation should include information that is available, formatted, and automated in order to increase efficiency, transparency and openness to control.

## CONTEXT

The Intelligence and Security sector (hereinafter I&S sector) in North Macedonia has undergone invaluable and estimable reform processes that have established a conceptual framework for liberal democratic functioning within the national security system and the protection of civil liberties and rights. Unlike before, contemporary legislation offers room for improved oversight and greater accountability and transparency. Nevertheless, the trajectory of reforms demands a dynamic and incessant process with the inclusive and comprehensive involvement of all relevant stakeholders.

This roadmap is premised on the fact that there are no established indicators or specific, objective metrics to measure the transparency, accountability and effectiveness of the I&S sector. In absence of such indicators, the resort to loosely defined or self-defined metrics to attest/imply that transparency and accountability are being upheld, as noted in the conclusions of the nominal group discussion.

### Methodological Approach

For the purposes of research and indicator development, a combined qualitative methodology was employed over a period of six months.

- **Contextual (preliminary) study** combining two methodological approaches: a *desk analysis*, and *qualitative analysis* through direct, semi-structured interviews and open-ended questionnaires with representatives from intelligence and security institutions and members of the Parliamentary security and intelligence committees in North Macedonia.
- **Qualitative analysis via nominal-group technique workshop (NGT WS)** discussions through customized scenario-based exercise. This multi-stakeholder approach enabled confronting issues through constructive problem-solving and collaborative brainstorming by representatives of intelligence and security institutions and independent actors (representatives from CSOs, media and academic community) and helped exchange reflections and stimulated testing of the established practices. The discussion generated ideas, prioritized issues and tested the multi-stakeholder problem-solving for matters of common interest.

The study aimed to put an emphasis on the current challenges and functions in the intelligence and security sector through several variables including the level of provision of information to the general public, the potential of information and communication technologies (ICTs) to enhance good Intelligence and Security sector governance, opportunities for cross-sectoral learning and norms transfer, as well as the use of digital tools to improve transparency and accountability.

## **THE MAIN CHALLENGES ASSOCIATED WITH ENSURING TRANSPARENCY AND ACCOUNTABILITY IN DIGITAL AGE IN NORTH MACEDONIA**

The research and in-depth analysis identified a handful of distinct challenges correlated with the digital ecosystem and the imperative for reform, which can be summarised as follows:

- The duality and the disruptive nature of some of the emerging technologies accelerate the process of power redistribution and with that, affect established processes of good governance nested under the liberal framework of accountability and transparency.
- Different conceptual set-ups in the digital sphere (which is horizontal and depends on end users) and the physical world (which is vertical top-down enshrined under the social contract theory of governance) put unprecedented tensions on the balance between national security and civil liberties;
- The idea on which the whole digitalization is developed is not built for accountability, but for communication, hence the principles of openness, connectedness, and interdependence all intrinsic to digitalization override the geospatial assumptions on which the states and the rules and principles that they have created were designed;
- Information sharing and operating in a vacuum without synchronization of the legislation, procedures and resources remain a challenge in a sensitive environment;
- Socio-economic and political factors that shape the specificity of the context impose confines in technology-enabled security sector reforms;
- The personal (effect of closed circles) and administrative barriers often fail to keep the pace with the trajectory of the reforms.

## **RECOMMENDATIONS FOR BETTER EFFICIENCY, TRANSPARENCY AND ACCOUNTABILITY OF THE INTELLIGENCE AND SECURITY SECTOR OF NORTH MACEDONIA**

- 1) The Intelligence & Security sector in North Macedonia needs to be built on professional merits and standards anchored under the liberal democratic framework, in a transparent and accountable manner;
- 2) The Intelligence & Security Sector in North Macedonia needs to be subject to oversight that is complete, consistent and systematic. Oversight should be complete in terms of ‘who’ conducts the oversight, ‘when’ the oversight is conducted and ‘how’ the oversight bodies perform the oversight. When it comes to “who” conducts the oversight, this need to include the government, parliament, the judiciary, and a specialized (non-parliamentary, independent civilian-based) body. The civil society should play an active role as well, presuming that it is independent and properly informed. When it comes to “when” the oversight needs to be performed, it should include prior, ongoing, and after-fact oversight. In terms of “how” the oversight should be performed/conducted, the oversight must focus on the reviews of lawfulness and effectiveness. In terms of “what” the oversight must consider, it should be designed and built to cover all stages of the Intelligence & Security cycles of work. This means that the oversight considers the data collection, data storage, data selection and data analysis.
- 3) The Intelligence & Security sector in North Macedonia needs to be subject to oversight that is fully funded, trained and equipped. Using excuses such as the complex legislature is just hurting the image and with that ability for professional performance of the sector and undermines public trust. Government should ensure that oversight bodies have proper funding, programs for capacity building and relevant resources to conduct oversight.
- 4) The normative route must be intrinsically tied with pre and post legislative scrutiny of intelligence and security laws regarding their pragmatic implementation to safeguard more efficient and consistent legislative, normative and regulatory framework.



## RECOMMENDATIONS FOR BETTER EFFICIENCY, TRANSPARENCY AND ACCOUNTABILITY OF THE INTELLIGENCE AND SECURITY SECTOR OF NORTH MACEDONIA

- 5) The Intelligence & Security sector in North Macedonia needs digitalization that will enhance its performance, and effectiveness but will also increase transparency, accountability and populace trust. The digitalization of court orders is expected to increase efficiency in the electronic exchange of data and information that consequently will reduce time and increase public confidence. But risks should be considered as well. The adequacy of digital protection via relevant encryption techniques is crucial for smooth and effective completion and fruition of the ongoing digitalization processes. This entails multi-stakeholder approach and cross-institutional learning among relevant stakeholders in building strong and secure digital security sector ecosystem.
- 6) While embracing digitalization Macedonian Intelligence & Security sector must consider the convergence challenges that accompany the process and build its capacities (human capital, technologies and processes) anchored to good liberal democratic practices that favor accountability and transparency.
- 7) The security sector actors should consider digitalization in a broader sense which can provide greater transparency by utilizing digital technology for more accessible website databases with relevant documents (legislative and policy) that would make the civilian oversight easier to be performed. It will make institutions more inclusive and open to oversight.
- 8) The Intelligence & Security sector in North Macedonia must consider capacity-building efforts for improving strategic communication capabilities, public outreach and building trust with the civilian sector and the media.
- 9) The Intelligence & Security sector in North Macedonia must consider the cultural shift from risk aversion to risk management to meet the ever-needed reform requirements with all the associated benefits and risks.
- 10) The Government should consider good democratic practices of enhancing the civil sector's role in the overall oversight of the Intelligence & Security sector. This may involve raising awareness and capacity-building activities that will improve the civil sector's ability to perform such task.

## PERFORMANCE INDICATORS FOR INTELLIGENCE & SECURITY SECTOR FOR EFFICIENCY, TRANSPARENCY AND ACCOUNTABILITY

These indicators are designed to serve the security leadership, decision-makers, and employees in the intelligence and security institutions as **reliable and objective metrics** in measuring/verifying the performance (achieved results) and systematically to address the gaps in relation to the principles of good governance of the security sector. They can also serve the independent actors (CSOs, media and academic community) in exercising their civilian control functions. The indicators are divided into three categories: 1) Effectiveness and Efficiency, 2) Transparency, and 3) Accountability. They are both quantitative (with predetermined value) and qualitative (descriptive). The indicators are context-specific, tailored to reflect the local reality and are based on the primary data (direct input via structured method of nominal group discussions, open-ended questionnaires, and individual interviews with representatives of the intelligence and security sector in North Macedonia, oversight bodies and independent actors).

Performance Indicators for Intelligence & Security Sector for Efficiency, Transparency and Accountability (reliable and objective metrics)						
Sector Concerned	Indicator	Type	Reference value (for quantitative indicators)	Source of verification	Priority	Action needed
<b>Category 1: Effectiveness and Efficiency</b>						
Operational Technical Agency (OTA)	Quality of systems, tools, and personnel in place to support digitalization	Qualitative	/	Annual reports	High	Procedural strengthening; technical support; removal of administrative barriers
Operational Technical Agency (OTA)	The digitalized system for processing court orders related to special investigative measures (SIM) is operational and functional	Qualitative	/	Court Reports	High	Reduction of administrative barriers
Intelligence and security sector in general	Percentage of staff trained to effectively use digital tools relevant to their roles in supporting intelligence activities	Quantitative	>30%	Evaluation reports; training sheets	Medium	Capacity building activities; vocational trainings
Intelligence and security sector in general	Level of optimization of personnel/workforce (less staff and time needed to provide service)	Qualitative	/	Direct discussions or semi-structured interviews with staff	Medium	Facilitation of procedures; technical support; cross trainings programmes
Intelligence and security sector in general	Number of oversight reports with progress noted	Quantitative	>3 per year	Oversight reports	High	Awareness raising meetings and trainings



Performance Indicators for Intelligence & Security Sector for Efficiency, Transparency and Accountability (reliable and objective metrics)						
Sector Concerned	Indicator	Type	Reference value (for quantitative indicators)	Source of verification	Priority	Action needed
<b>Category 2: Transparency</b>						
Intelligence and security sector in general	Legislative and policy documents and regulations are easily accessible and publicly available	Qualitative	/	Official websites	High	Awareness raising campaigns; policy dialogue
Intelligence and security sector in general	A transparent organizational structure is in place (who, what, why)	Qualitative	/	Official websites	Medium	Awareness raising campaigns; policy dialogue
Intelligence and security sector in general	Adequate information about budgetary appropriations (financial policies, budget, spending)	Qualitative	/	Official websites	High	Awareness raising campaigns; policy dialogue
Intelligence and security sector in general	Number of interviews, public statements and press briefings provided by the intelligence and security leadership	Quantitative	>3 per year	Official websites, internet, mainstream media	High	Awareness raising campaigns; policy dialogue
Intelligence and security sector in general	Range and variety of communication channels utilized for communication with public	Qualitative	/	Official websites, internet, mainstream media	Medium	Awareness raising campaigns; policy dialogue
Intelligence and security sector in general	Number of cooperation initiatives with independent actors raised	Quantitative	>3 per year	Registry of cooperation agreements	Medium	Improving outreach and civilian control

**Performance Indicators for Intelligence & Security Sector for Efficiency, Transparency and Accountability (reliable and objective metrics)**

Sector Concerned	Indicator	Type	Reference value (for quantitative indicators)	Source of verification	Priority	Action needed
<b>Category 3: Accountability</b>						
Intelligence and security sector in general	<b>Accountability reports are regularly available and accessible</b>	Qualitative	/	Official websites; periodic reports; direct discussions with security leadership	High	Integrity trainings
Intelligence and security sector in general	<b>The level of hard accountability (answerability and mechanisms for personal liability) is clearly defined</b>	Qualitative	/	Internal regulations/ reports (if publicly available); oversight reports	High	Development of system-oriented strategies; Awareness raising
Intelligence and security sector in general	<b>Vertical accountability in place: participation and inclusiveness in decision-making, openness to democratic oversight and control</b>	Qualitative	/	Research reports (interviews, focus groups); assessment reports by independent actors	Medium	Support for independent monitoring activities, watchdog efforts, public scrutiny
Intelligence and security sector in general	<b>Horizontal accountability in place: better communication, coordination and reporting between institutions, sectors, and agencies</b>	Qualitative	/	Research reports (interviews, focus groups); assessment reports by independent actors	Medium	Peer support, coaching, exchange visits; clear standards for reporting
Intelligence and security sector in general	<b>Level of public confidence in intelligence and security services</b>	Quantitative	>30 %	Surveys, public opinion polls	High	Strengthening the communication between I&S sector actors and the public

## Concluding Remarks

The nominal group discussions identified several important considerations pertaining to the overall perceptions of Intelligence and Security services. Representatives from both security institutions and independent actors share the view that imparting information to the public is an important aspect of building transparency and accountability. However, the sensitivity of certain actions inhibits the institutions' ability to be fully open and transparent.

The primary associations made by representatives of independent actors (CSOs, media, and the academic community) when discussing intelligence and security institutions and their operations are rigidity, bureaucracy, and closedness. These actors still perceive intelligence and security services in a traditional manner, viewing them as entities primarily engaged in obscure or clandestine operations rather than as accessible security providers.

On the other hand, the representatives of the institutions hold a more moderate view on this issue. They believe that with appropriate communication strategies and information campaigns, the intelligence-security community can establish closer ties with the public and enhance trust in intelligence and security institutions.

Notwithstanding, most participants agreed that there is a lack of knowledge and understanding among public regarding how to hold the security sector accountable. Nevertheless, they concurred that the democratization of the security sector should be based on the principles of participation, openness to public control and transparency, which, among other things, will strengthen the democratic legitimacy of the security institutions.

When it comes to functionality of the work, most participants are positioned that performance of the security sector would be much higher if the security community relies on digital tools based on good practices, human rights protection and well-defined accountability mechanisms. It was inferred that although there is a significant progress in the recent years in terms of enhanced transparency and accountability of the intelligence and security sector, however, there are still shortcomings and loopholes in the legislation in ensuring full transparency and availability of information, given that most of the legislative framework is either non-precise or lacking specific provisions that regulate the transparency and accountability guarantees. Although the degree of commitment is not even in all security institutions, the need to intensify the efforts to fill the gaps in accountability and transparency are more than evident and they should be particularized based the institutional needs.

The above indicators will serve the intelligence and security sector actors to monitor the progress of effectuating the principles of good security sector governance, but also the independent actors (CSOs, media and academic community) in exercising their civilian control functions. The monitoring of the indicators is not time-bound and requires consistent monitoring but should be subject to regular review and revision in line with the contextual changes.

