TRANSPARENCY INTERNATIONAL
Defence & Security

# UNLOCKING ACCESS:

## BALANCING NATIONAL SECURITY AND TRANSPARENCY IN DEFENCE

**Transparency International (TI) is the world's leading non-governmental anti-corruption organisation, addressing corruption and corruption risk in its many forms through a network of more than 100 national chapters worldwide.**

**Transparency International Defence and Security (TI-DS) works to reduce corruption in defence and security sectors worldwide.**

Authors: Stephanie Trapnell, Yi Kang Choo

Contributors: Léa Clamadieu, Irasema Guzman Orozco, Matthew Steadman

Reviewers: Anamarija Musa, Atzimba Baltazar-Macías, Francesca Grandi, Alexander Knapp

Editor: Michael Ofori-Mensah

Design: Colin Foo

With thanks to TI-Malaysia, TI-Armenia, TI-Guatemala, TI-Niger/ANLC, and TI-Tunisia/IWATCH for their contributions to the case studies. We would also like to thank several civil society experts and academics who participated in our expert interviews, including Artur Sakunts, Genya Petrosyan, and Edgar Khachatryan.



With special thanks to the Ministry of Foreign Affairs of the Netherlands for its generous support. The contents of this publication are the sole responsibility of Transparency International Defence & Security and can in no way be taken to reflect the views of the Ministry of Foreign Affairs of the Netherlands.

Ministry of Foreign Affairs of the Netherlands

Published December 2024

# CONTENTS

## List of Figures



## List of Tables

## List of Tables



## List of Boxes

# EXECUTIVE SUMMARY

Despite widely agreed international standards for access to information in the defence and security sector, transparency remains insufficient to ensure accountability. National security exemptions are frequently applied in vague and undefined ways, limiting the release of precise, timely and detailed information that is crucial for understanding how government is functioning and protecting public interest, especially in areas as fundamental as national security.

Information exchange within government facilitates various types of accountability - from parliamentary scrutiny of executive decisions, to audits of the government's use of public funds as well as disciplinary sanctions for public officials. More importantly, information disclosure to the public by government bodies also forms the foundation for meaningful citizen engagement and accountability. This is true not just for voting and activism, but for interest in the policies that determine the course of daily life, including whether the security forces are absent, overmilitarised, or well-balanced.

Legitimate national security interests are best safeguarded when the public is well-informed about government activities, including those undertaken to ensure safety and protection. Access to information enables public scrutiny of government action and facilitates public contribution to policymaking and national debate, thus serving as a crucial component of genuine national security, democratic participation, and sound policy formulation. Access to information is also a specific aspect of governance that involves the intentional disclosure of information. These policies require the release of information that is relevant to the public, and is also accessible, accurate and timely.

This report provides an overview of the state of defence transparency and access to information related to defence and security sectors worldwide, drawing on the Government Defence Integrity (GDI) database on institutional integrity and corruption risk. In light of increasing global military spending (with a new world record of $2.443 trillion recorded in 2023) the overarching focus is on access to defence-related financial information, as transparency and appropriate oversight of defence finances remain critical for public accountability.

Further, this report also includes a review of global standards for transparency that apply to the defence sector, specifically the UN Convention Against Corruption (UNCAC) and the Global Principles on National Security and the Right to Information (or Tshwane Principles). This is coupled with specific exploration of five country cases (Armenia, Guatemala, Malaysia, Niger, and Tunisia) and insights from their legal frameworks and implementation experiences. It concludes with recommendations for good practice to enhance access to information.

# KEY INSIGHTS

The 2013 Global Principles on National Security and the Right to Information (or Tshwane Principles) outline specific guidelines for access to information related to national security and defence sectors. While they are not binding, they serve as internationally agreed guidance and standards for countries in how to appropriately balance information access with national security concerns.


In Armenia, Guatemala, Malaysia, Niger, and Tunisia (the five case studies in this report), the most common obstacle to effective access to information in the defence sector is the security classification scheme for information.

Only two of those countries have balancing tests in their laws. These tests are critical for the appropriate withholding of sensitive information, as they require officials to weigh the benefit of disclosure against the potential harm to protected interests.

Another means of countering the pressure to withhold information is the regular, proactive release of information that is recognised as being in the public interest. This includes a range of financial information, including budgets, income, expenditures, oversight reports, and procurement.

Good practices for access to information enable greater accountability for the defence sector. Issues that matter for good practice include: legal exceptions to disclosure, length of classification periods and classification procedures, archival processes, administration and oversight, and proactive release of information.

The absence of *publicly* available information denies civil society organisations access to fundamental aspects of defence policymaking and finances that are inherently part of the vertical process of democratic accountability. This lack of transparency carries severe consequences for the defence sector: it obstructs civic engagement in defence matters, impedes institutional accountability, and threatens the legitimacy of the defence establishment.

# SECTION 1

# LEGAL AND POLICY FRAMEWORKS FOR ACCESS TO INFORMATION IN DEFENCE

## Defence Transparency and Access to Information

Information and transparency[1] are critical elements of democracy. They underpin political processes, citizen participation, proper government functioning, and ultimately, the protection of human rights. Without accurate information, government falters. In the midst of secrecy, corruption flourishes. As noted by one transparency scholar, "[t]he weakening, erasure, suppression, and corruption of transparency starves democracy of its oxygen – the free flow of information."[2]

Information exchange within government facilitates various types of accountability, from parliamentary scrutiny of executive decisions, to audits of the government's use of public funds, to disciplinary sanctions for public officials. Information disclosure to the public is the foundation for citizen engagement. This is true not just for voting and activism, but for interest in the policies that determine the course of daily life – whether there is sufficient electricity to heat homes, whether the public schools have enough resources, whether the security forces are absent or overmilitarized, and for the purposes of this report, information is crucial for understanding how the government is ensuring national security.

Legitimate national security interests are best protected when the public is well-informed about government activities, including those undertaken to protect national security. Access to information enables public scrutiny of government action and facilitates public contribution to policymaking and national debate, thus serving as a crucial component of genuine national security, democratic participation, and sound policy formulation.[3]

This report aims to provide an overview of the state of defence transparency and access to information worldwide, using the Government Defence Integrity Index (GDI) database on institutional integrity and corruption risk. It also includes a review of global standards for transparency that apply to the defence sector. This is coupled with specific exploration of five country cases and insights from their legal frameworks and implementation experiences. It concludes with recommendations for good practice to enhance access to information.

## Methodology

This report builds on three sources of evidence: desk review, key informant interviews, and the 2020 Government Defence Integrity Index (GDI) (see Box 1).

An in-depth review was conducted across the relevant legal and policy documents on access to information and transparency in the defence sector, including relevant global standards. The global analysis of specific issues related to defence transparency utilised data from the 2020 GDI.

In light of increasing global military spending, this report also focuses on defence finances because they are critical for civic engagement and public accountability, as highlighted by the Tshwane Principles and open government initiatives that prioritise financial transparency. Information on budget allocations, expenditures, and procurement is particularly critical, given the high risks of corruption and mismanagement in these areas. Unlike information linked to defence personnel and military operations, which are constrained by confidentiality and security concerns, defence financial information is less restricted, making it a practical and impactful starting point for advancing accountability and good governance in the sector.

1 Transparency International defines transparency as the "characteristic of governments, companies, organisations and individuals of being open in the clear disclosure of information, rules, plans, processes and actions". See https://www.transparency.org/en/corruptionary/transparency

2 Michener, Gregory. "Transparency Versus Populism." *Administration & Society* 55, no. 4 (April 1, 2023): 671–95.

3 "The Global Principles on National Security and the Right to Information (Tshwane Principles)." Open Society Justice Initiative, 2013.

Case studies were completed for five countries: Armenia, Guatemala, Malaysia, Niger, and Tunisia. The case studies were selected from a diverse group of countries across different continents, each at varying stages of progress in advancing access to information. The selection was also guided by the advocacy priorities of national TI Chapters with a keen interest to explore tailored recommendations for further reforms in access to information within their respective national defence and security sectors.

Research for the cases was compiled through interviews with local experts in each country (e.g., CSOs, government officials, journalists, lawyers), review of policy reports and media investigations, and updates of GDI data as confirmed by Transparency International (TI) national chapters.

**In light of increasing global military spending, this report also focuses on defence finances because they are critical for civic engagement and public accountability, as highlighted by the Tshwane Principles and open government initiatives that prioritise financial transparency.**

Selected case study countries face particular challenges based on their national contexts:

- **Armenia:** Decades of conflict with Azerbaijan over Nagorno-Karabakh have driven high defence spending, but access to defence information has been severely restricted by a 2024 state secrets law, overriding the freedom of information law.
- **Guatemala:** Corruption has plagued Guatemala for a decade, but the 2024 administration of Bernardo Arévalo, focused on anti-corruption, and efforts to strengthen transparency and accountability in government have been revitalised.
- **Malaysia:** Despite a peaceful power transition in 2018, governance reforms have stalled, with the Official Secrets Act 1972 severely limiting access to information.
- **Niger:** The coup d'état in 2023 escalated violence, cut foreign aid, and curtailed democratic rights, while the limited access to information framework also lacks meaningful implementation and enforcement mechanisms.
- **Tunisia:** Democratic backsliding since 2021 has reduced government transparency, though a strong access to information law exists, with defence-related information often kept confidential.

# KEY INSIGHTS

Access to information is a specific aspect of governance that involves the intentional disclosure of information. These policies require the release of information that is relevant to the public, and is also accessible, accurate and timely.

The 2013 Global Principles on National Security and the Right to Information (or Tshwane Principles) outline specific guidelines for access to information related to national security and defence sectors. While they are not binding, they serve as internationally agreed guidance for countries in how to appropriately balance information access with national security concerns.

Under well-formulated Right to Information (RTI) laws, when requests are made for protected information, the "public interest test" is triggered. This requires authorities to balance the potential harm of disclosure against the public interest in disclosure, which is also called a "balancing test." If information is withheld there should be procedures (accessible to all) that allow for substantial review by independent bodies.

As a fundamentally public document that sets out spending priorities and the allocation of public funding, budgetary information on defence should be readily available. The same is true of defence expenditures and income, particular income streams that are off-budget or through private enterprise.

Enhancing transparency and access to information on the entire procurement cycle can significantly reduce corruption risk, facilitating scrutiny by oversight institutions, increasing external involvement in the procurement planning process, and mitigating opportunities for corruption at key junctures of the process.

A critical factor in robust civic engagement in defence matters is the transparency of planning processes, specifically before actions are taken, rather than after. This includes consultations on white papers, defence strategies and policy, acquisition planning, and procurement processes.

The lack of transparency around defence lobbying is a major corruption vulnerability, as undue influence from the private sector in both policymaking and procurement has been found to increase corruption risks in the countries with powerful defence industry players.

**Box 1: The Government Defence Integrity Index (GDI)**

## The Government Defence Integrity Index: good practice standards for institutional integrity

Through extensive experience working on the specificities of anti-corruption in the typically secretive and opaque defence and security sectors, TI-DS developed a unique tool that captures comprehensive and in-depth information on the quality of institutional checks on corruption in defence sectors. The GDI covers five specific areas of corruption risk[4], providing both a gauge of corruption vulnerabilities within defence institutions and a snapshot of the quality of defence sector governance. The GDI 2020 therefore provides a unique dataset not only for assessing risk, but also for assessing institutions, policies, and practices against baseline good practice standards.

## The Importance of Information Access

The defence sector is frequently cited as one of the most opaque areas of government activity, despite being an area of exponential government expenditure.[5] This lack of transparency undermines sound financial management of the sector and creates a high vulnerability to corruption, especially in relation to procurement and defence sector expenditure more broadly.[6]

While transparency is considered a general state of openness, access to information has a narrower scope[7]—it is the *public availability of information held by the government*. This information is disclosed in the public interest regardless of whether it has historically been considered "secret," as long as the benefit of public interest is seen to outweigh the harm of disclosure. In countries with a legal framework establishing the right to information, this balancing test of harm vs public interest forms the core of decision-making around sensitive areas such as national security, trade secrets, and public health (including privacy concerns).

**Box 2: Definition of transparency**

**Transparency** facilitates a process of opening government by encouraging citizen participation and various forms of accountability. It is a broad approach to governance that entails openness and integrity in the business of government.

Access to information is thus a specific aspect of governance that involves the intentional disclosure of information by the government from its own repositories. It is often conflated with right to information laws (or freedom of information laws), as these laws serve as the legal grounds for access to information policies throughout government. But with the emergence of transparency and openness as global norms, access to information has evolved to include more than reactive release of information.[8] Specialised transparency policies now require the proactive disclosure of budgets and expenditure information, conflicts of interest by public officials, procurement data, and beneficial ownership of businesses. There are also open data mandates and open government initiatives that span the whole-of-government.

4 Transparency International Defence and Security, Government Defence Integrity Index (GDI) 2020 Global Report: Disruption, Democratic Governance, and Corruption Risk in Defence Institutions (London: Transparency International UK, 2020).

5 World military expenditure increased for the ninth consecutive year in 2023, reaching a total of $2443 billion. The 6.8 per cent increase in 2023 was the steepest year-on-year rise since 2009 and pushed global spending to the highest level ever recorded. Tian, Nan, Diego Lopes da Silva, Xiao Liang, and Lorenzo Scarazzato. "Trends in World Military Expenditure, 2023." Stockholm International Peace Research Institute (SIPRI), April 2024.

6 Perlo-Freeman, Sam. 'Transparency and Accountability in Military Spending', Stockholm International Peace Research Institute (SIPRI), 3 August 2016.

7 Access to information is often equated with transparency and is regularly used as a proxy for transparency because it can be measured more easily, as well as being regulated through RTI laws.

8 Schnell, Sabina. "To Know Is to Act? Revisiting the Impact of Government Transparency on Corruption." *Public Administration and Development* 43, no. 5 (2023): 355–67.

**Box 3: Definition of access to information**

**Access to information** is a specific aspect of governance that involves the intentional disclosure of information. These policies require the release of information that is relevant to the public, and is also accessible, accurate and timely.

Access to information policies require the release of information that is relevant to the public, and is also accessible, accurate and timely. This means that information is not presumed "secret" simply because of tradition or authority, but according to clear rules of classification that consider the public interest of disclosure.[9] It means that information and data is both digitally accessible through online publication, and machine-readable as basic spreadsheet and data files. It entails clarification about government processes, rules, and decisions, as well as proactively disclosing information rather than waiting for information requests to trigger release.

In short, the responsibility of administering access to information involves not only *disclosure*, but also *clarification* and *dissemination* of information to stakeholders, as well as a *commitment* to information integrity. These standards are even more important for the defence sector, as it has historically been an area of extreme secrecy, with little opportunity for non-specialists to understand its scope, or for the legislature to exercise appropriate oversight.

Access to information is a vital tool for combating corruption, strengthening institutional integrity, and fostering trust and legitimacy in government actions. It enables external oversight of government by legislators, civil society and the media, increasing accountability of political decision-making and institutional practice. It enables informed participation of experts, the public, and civil society in public debates and development of policy and law. And it brings corruption risks – and actual incidents of corruption – to light, facilitating the push for accountability and reform.[10]

## Global Standards

Global initiatives and norms on transparency have proliferated in the past decades, as the idea of openness has become recognised as not only an integral component of democracy, but as a basis for business integrity in the private sector. These developments have translated into a widespread acceptance of transparency in government and public administration, particularly through open budget and e-procurement initiatives, even within traditionally secretive defence sectors. But norms around 'defence sector exceptionalism' still serve to block access to critical information about defence planning and spending. Even mundane decision-making around non-strategic acquisitions, personnel hiring and promotion processes, and information classification and management are held back for so-called confidential purposes.

**Box 4: UNCAC standards on transparency**

**Article 10 of UNCAC requires that governments enhance transparency in public administration as a means of combatting corruption by:**

(a) Adopting procedures or regulations allowing members of the general public to obtain, where appropriate, information on the organisation, functioning and decision-making processes of its public administration and, with due regard for the protection of privacy and personal data, on decisions and legal acts that concern members of the public;

(b) Simplifying administrative procedures, where appropriate, in order to facilitate public access to the competent decision-making authorities; and

c) Publishing information, which may include periodic reports on the risks of corruption in its public administration

**Article 13 states that member countries must take appropriate measures to promote the active participation of individuals and groups in the fight against corruption by:**

(a) Enhancing the transparency of and promoting the contribution of the public to decision-making processes;

(b) Ensuring that the public has effective access to information;

(c) Undertaking public information activities that contribute to nontolerance of corruption, as well as public education programmes, including school and university curricula;

9 The general rule is that disclosure is the default, except when a legitimate interest in protecting information outweighs the right to know in a given case.

10 Transparency International, Defence & Security. "Access to Information in the Defence Sector: The Balance between Secrecy and Transparency." TI-DS Factsheet. London, 2023.

Within global instruments such as the 2005 United Nations Convention Against Corruption (UNCAC)[11]—the only legally binding universal anti-corruption instrument—there are exceptions made for national security that can be interpreted excessively and broadly.

Articles 10 and 13 of UNCAC specifically mandate the disclosure of information to combat corruption, but follow this with a broad exemption for national security: the "freedom to seek, receive, publish, and disseminate information concerning corruption" is subject to restriction "for the protection of national security, public order, or public health." However, there is no further clarification provided on the scope and definitions of these exemptions, nor highlighting the need for a robust balancing test of harm against public interest.

### Box 5: Origins of the Tshwane Principles

**The Global Principles on National Security and the Right to Information (or "Tshwane Principles")** address the question of how to ensure public access to government information without jeopardising legitimate efforts to protect people from national security threats.

These Principles were drafted by 22 civil society organisations and academic centres, facilitated by the Open Society Justice Initiative, in order to provide guidance to those engaged in drafting, revising, or implementing relevant laws and policies.

Based on international and national law and practices, and more than two years of consultation around the world with government actors, the security sector and civil society, they set out concrete guidelines on the appropriate limits of secrecy, protections for whistleblowers, the parameters of the public's right to information about human rights violations and other issues.

By contrast, the 2013 Tshwane Principles outline specific guidelines for access to information related to national security and defence sectors. They are not binding, however, and serve only as guidance on how to appropriately balance information access with national security concerns.

Transparency in the defence sector is always a balance between state secrecy and the public's right to information. In certain circumstances, there will be a need to keep information secret in order to protect legitimate national security interests, or in the case of procurement processes, to protect the trade secrets of participating defence companies (e.g., new or advancing technologies). But in many laws, national security is vaguely defined. National legislation can refer interchangeably to national security, state security, public security, public safety, national defence, national interest, state secrets, security of the realm, of the republic and so forth.[12] Lack of definitional precision and international standardisation create a high risk of overuse that can conceal misconduct or mismanagement, or simply overburden the ministry of defence with masses of classified documentation that has little to do with protecting national security.

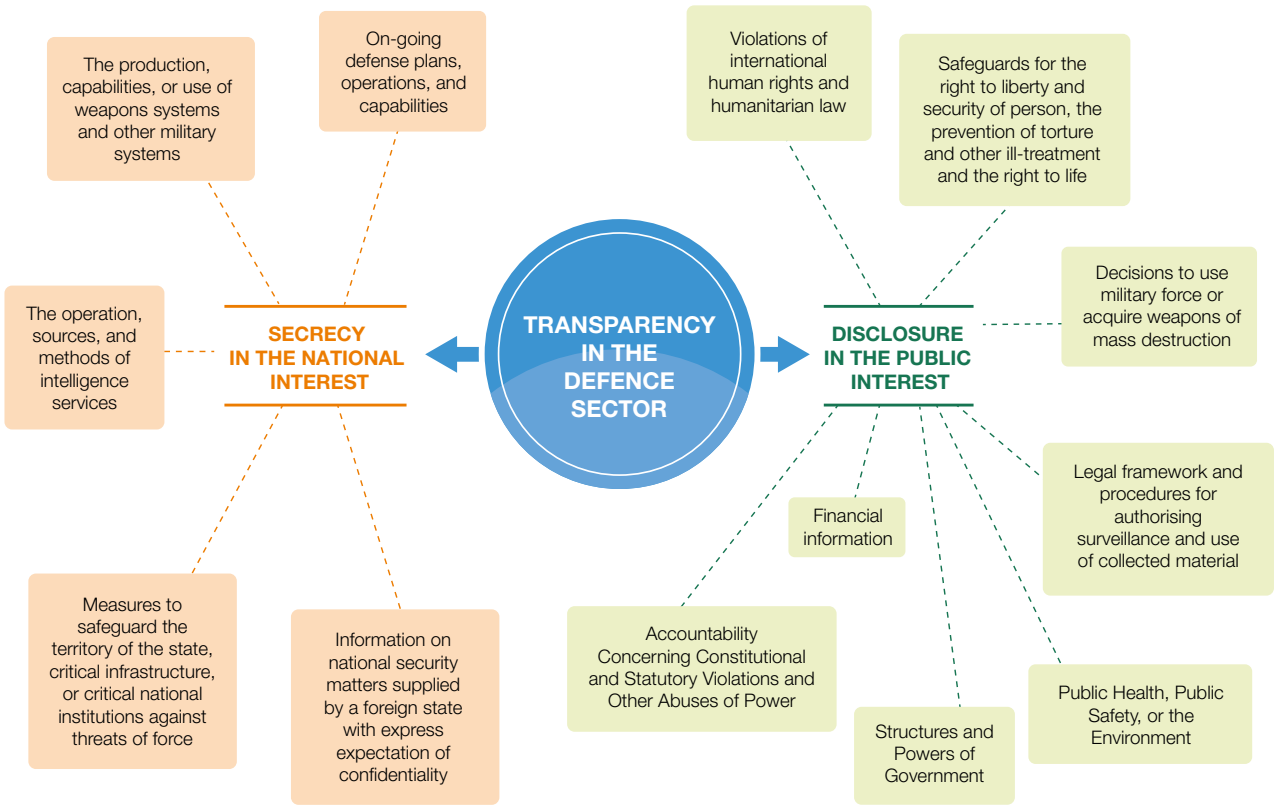
The Tshwane Principles clearly identify the classes of information that have grounds for withholding in the national interest, and those that have an overriding public interest in disclosure (See Figure 1). In addition, the principles outline rules for classification and declassification, oversight bodies, asset disclosures by public officials, and whistleblowing.

**TRANSPARENCY IN THE DEFENCE SECTOR IS ALWAYS A BALANCE BETWEEN STATE SECRECY AND THE PUBLIC'S RIGHT TO INFORMATION**

11 UNCAC adopts a comprehensive approach to tackling corruption, emphasising the importance of preventive measures such as access to information, while also including criminalization and law enforcement, international cooperation and asset recovery. It came into force in 2005, and has been ratified by 140 member countries.

12 Cardona, Francisco. "Access to Information and Limits to Public Transparency." Guides to good governance No 4. Oslo: Centre for Integrity in the Defence Sector, 2016.

**Figure 1: Legitimate grounds for withholding or disclosing information according to the Tshwane Principles (2013)**




## GDI 2020 Findings

The Government Defence Integrity (GDI) index evaluates the corruption risk of defence sectors on a set of 77 questions spanning policy processes, finances, personnel, operations, and procurement.[13] Several areas of disclosure outlined in the Tshwane Principles are included in GDI indicators, specifically: disclosure of financial information, structures and powers of government, and to a limited extent, decisions to use military force or acquire weapons of mass destruction. This section presents the landscape of information disclosure practices as reflected in the 2020 GDI, with a view to better understanding both good practices and governance gaps.

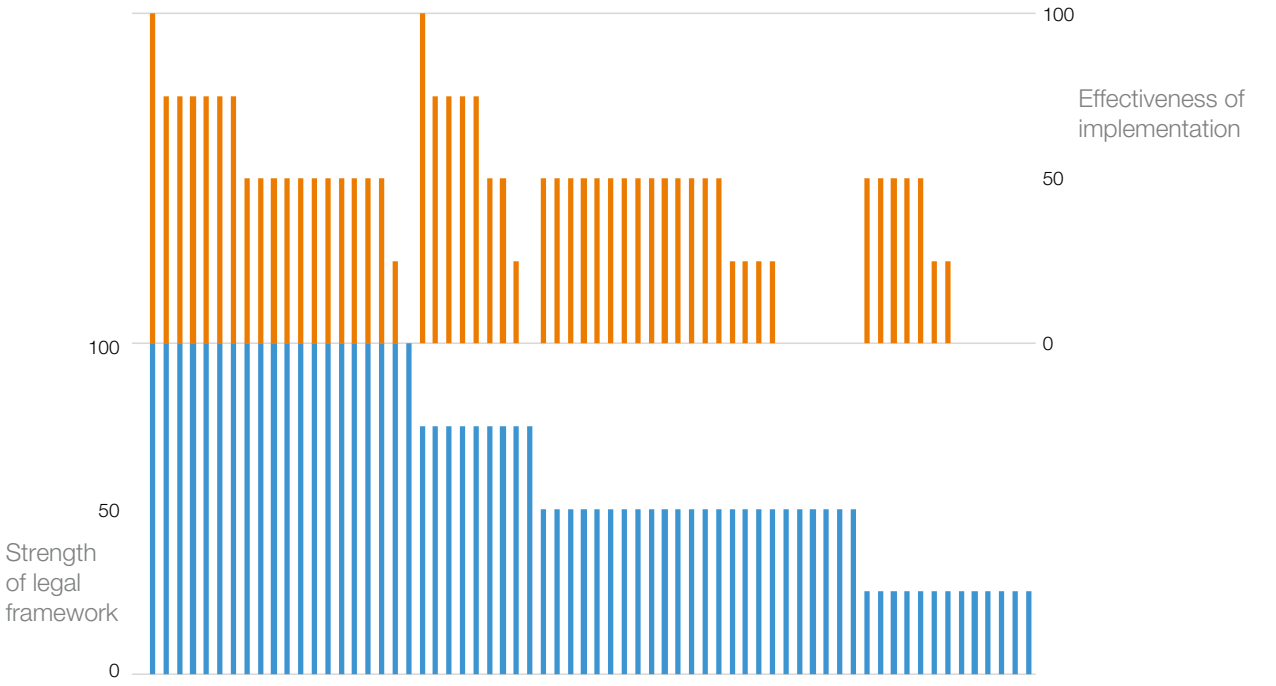
## The Right to Information and Information Classification

The right to information (RTI) empowers citizens to obtain information held by public bodies with exceptions specified in the law. It encompasses a legal right to seek, receive and impart information. The legal and policy framework surrounding RTI systems sets out the parameters for requesting information from government entities, which is released when specifically requested.

The 2020 GDI findings reveal that over a third of countries with critical risk in transparency have no RTI law, and of 86 countries assessed in the index, nearly 15% do not have an information law. Moreover, it is rare for a country with the highest score for the strength of its RTI legal framework to gain a similarly high score for its implementation (Figure 2).

13 https://ti-defence.org/gdi/

**Figure 2: Gaps in right to information legal frameworks for defence-related information**




Countries also struggle with their information classification frameworks, either because these were weakly conceptualised, or poorly implemented. Information classification is a means of assessing the level of protection that information should be given, according to the requirements laid out in law, or in cases where there is no law, according to internal policies. The objective of protecting information is to prevent the disclosure of information that would pose a significant threat to national interests, which is decided through a **harm test**. This information is then assigned a heightened level of protection, e.g., "secret" or "top secret". Figure 1 presents internationally-accepted norms for the kinds of security and defence information that would generate significant harm if released (Secrecy in the national interest).[14]

Information classification systems require the government to think critically about its own information assets, and the most effective and efficient means of handling transparency mandates. In fact, recent information classification frameworks in the United Kingdom and New Zealand deal less with secrecy and more with risk management and information security.[15] Ideally, the frameworks result in less time arguing against disclosure with external stakeholders, and in fewer documents that require secrecy classification.

Under well-formulated RTI laws, when requests are made for protected information, the "public interest test" is triggered. This requires authorities to balance the potential harm of disclosure against the public interest in disclosure, which is also called a **balancing test**. There is no simple metric for determining public interest in disclosure, as this depends on the legal and country context, as well as the circumstances of harm in question.[16]

Unfortunately, many countries have restrictive policies on the release of information related to national security. Specialised state secrets legislation often prohibits and criminalizes the disclosure of information and serves as the overriding or controlling law. The GDI Index reveals

14 Other areas of national interest that may be considered acceptable exceptions to disclosure include: international relations; public health and safety; the prevention, investigation and prosecution of legal wrongs; privacy; legitimate commercial and other economic interests; management of the economy; fair administration of justice and legal advice privilege; conservation of the environment; and legitimate policy making and other operations of public authorities. See https://www.rti-rating.org/. However, there are no internationally-accepted norms for exactly what would constitute an appropriate exception.

15 Heide, Marlen, and Jean-Patrick Villeneuve. "From Secrecy Privilege to Information Management: A Comparative Analysis of Classification Reforms." *Government Information Quarterly* 37, no. 4 (October 1, 2020): 101500.

16 For a more detailed discussion of the public interest test, see: Paterson, Moira, and Maeve McDonagh. "Freedom of Information and the Public Interest: The Commonwealth Experience." Oxford University Commonwealth Law Journal 17, no. 2 (July 3, 2017): 189–210 Cook, Meredith. "Balancing the Public Interest: Applying the Public Interest Test to Exemptions in the UK Freedom of Information Act 2000." London, England: The Constitution Unit Department of Political Science UCL (University College London), 2003.

that in some instances defence-related information was de facto exempt from disclosure, either because there was no harm test (i.e., no consideration of harm, only presumption), or because the harm test was limited to certain classes of information. In a majority of cases, there was no requirement at all to consider the public interest when restricted information was requested, which means that once information is classified as restricted, it remains so without question.

Principle 2 of the 2013 Tshwane Principles suggests that good practice is to precisely define "national security" in a country's legal framework, in a way that is "consistent with a democratic society." But this is a persistent challenge that demands regular, ongoing dialogue between government and citizens. It is also paramount that information classification frameworks are publicly available, so that citizens are aware of how information is managed and classified, and can advocate for reform if needed.

Some RTI laws mandate proactive release of information,[17] but more often, the regular release of information is specified in transparency and administrative policies that stipulate adherence to open government and open data initiatives.


**Box 6: Good practice in secrecy classification**[18]

**Good practice in secrecy classification legislation includes rules on:**

- any restriction on right to information must meet international legal standards, and be present in the applicable national legislation;
- the authority to withhold or classify information should be well defined and originated from a legitimate source of power, and be performed in line with procedures prescribed by published legal rules;
- information may be exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm;
- if information is withheld there should be procedures (accessible to all) that allow for substantial review by independent bodies.

**Rules on secrecy classification legislation should be supported by additional safeguards, notably:**

- Guarantees that no information be withheld from the public for an indefinite period;
- Classifications and decisions on withholding information must be justified in writing and information be properly archived for present and historical purposes;
- The law should provide for a public interest test, or even prohibiting non-disclosure of certain categories of information;
- There should be a maximum expiry time in every secrecy regime.

17 Darbishire, Helen. "Proactive Transparency: The future of the right to information? A review of standards, challenges, and opportunities". The World Bank Institute.

18 Foldes, Adam. "Classified Information: A Review of Current Legislation across 15 Countries & the EU." London: TI Defence & Security, 2015.

# Defence Finances: Budgets, Spending and Income

The budget is a key foundational document for defence. It establishes the financial basis for the delivery of defence functions and implementation of policies and priorities. By balancing competing objectives, it determines the strategic allocation of public resources to different defence functions, while also acting as a planning document that outlines key priorities for defence for a given financial year. Unfortunately, secrecy practices result in budgets that are vague, incomplete and superficial. Opaque budgeting without public input and oversight from responsible institutions exacerbates opportunities for corruption and can skew budget priorities to the benefit of private interests.[19]

While budget comprehensiveness is the highest scoring 'financial' indicator in the index, there are still significant issues with disaggregation. Often published budgets provide only topline figures, without sufficient clarity on how funding is being allocated across defence priorities. Naming conventions are not explained, or defence projects are distributed across multiple departments or programs. Fiscal figures lack clarity, making it impossible to determine the fiscal implications of defence budgeting priorities.

**Figure 3: Key Findings for Transparency in Defence Finances**

| GDI Transparency Indicators: Defence finances | Index average scores | Top Scorers for each budget indicator |
|---|---|---|
| Proposed budget has comprehensive coverage of defence functions | 53 | Argentina, Australia, Belgium, Brazil, Colombia, Denmark, Germany, Italy, Japan, Latvia, Norway, Philippines, Sweden, Switzerland, United Kingdom, United States |
| Published budget is disaggregated with explanations | 53 | Argentina, Denmark, France, Germany, Japan, Latvia, Netherlands, New Zealand, Norway, Portugal, South Korea, Spain, Sweden, Taiwan, Uganda, United Kingdom |
| Sources, amounts, and allocations of defence income (not from central government) are published | 45 | Australia, Bangladesh, Belgium, Brazil, Denmark, Finland, Georgia, Germany, Japan, Kosovo, Latvia, Malaysia, New Zealand, Norway, Poland, Portugal, South Korea, Spain, Taiwan, United Kingdom |
| Defence spending is published and disaggregated | 45 | Armenia, Denmark, Georgia, Germany, Ghana, Italy, Latvia, Mali, Netherlands, New Zealand, Nigeria, Norway, South Africa, United Kingdom, United States |
| Financial results of asset disposals are published and disaggregated | 29 | Belgium, Colombia, Estonia, Germany, Netherlands, Norway |

| Range of Scores | | | | | Corruption Risk |
|---|---|---|---|---|---|
| A | 83 | – | 100 | Very robust institutional resilience to corruption | Very low |
| B | 67 | – | 82 | Robust institutional resilience to corruption | Low |
| C | 50 | – | 66 | Modest institutional resilience to corruption | Moderate |
| D | 33 | – | 49 | Weak institutional resilience to corruption | High |
| E | 17 | – | 32 | Very weak institutional resilience to corruption | Very high |
| F | 0 | – | 16 | Limited to no institutional resilience to corruption | Critical |

19 Transparency International, Defence & Security. "GDI 2020 Global Report: Disruption, Democracy, and Corruption Risk in Defence Sectors." London: Transparency International UK, November 2021.

In many countries, there are also problems with public access to budgets: proposed defence budgets are not released at all, or with significant delay, thus preventing external inputs into budgeting processes and ensuring that the budgeting cycle is tightly executive-controlled and external involvement is kept at a minimum.

As a fundamentally public document that sets out spending priorities and the allocation of public funding, budgetary information should be readily available and if not, should be available to access via right to information legislation. However, in more than two-thirds of countries assessed in the GDI, there are unjustified refusals to share requested budgetary information, information is arbitrarily redacted, or it is simply impossible to access through information requests.

### Box 7: Good practice in budgeting and expenditure tracking

**Good practice in budgeting and expenditure tracking should include the following categories, at a minimum:**

- personnel (salaries, allowances, entitlements),
- military research and development,
- training,
- construction,
- procurement/acquisitions,
- maintenance of equipment,
- disposal of assets, and
- administrative expenses (Ministry of Defence or other services)

Furthermore, access to information on defence expenditures poses a significant challenge for a majority of countries in the index. Half of the countries in the index publish disaggregated data on actual expenditure, with very few proactively publishing disaggregated spending information that is accompanied by explanations. However, for other countries, spending figures are distributed across outlets. They may be released in annual reports from the ministry of finance or ministry of defence, or they may be disclosed in separate year-end reports by different departments. Monthly reports may include spending figures, but use different budgeting categories that do not correspond to the published budgets. In some cases, expenditures can only be tracked through individual contracts within the procurement system. In some cases, expenditures only appear in the following year's proposed budget, with no explanations or disaggregation. Nearly 30% of countries in the GDI database do not publicly report on actual defence spending. As a result, there is little clarity as to how these public funds are used in a given year, which fuels unaccountable defence spending and the potential wasting of valuable and scarce public resources.

Confidential income streams also present a grave corruption risk for defence sectors. Sources of funding outside of central government allocation are already highly vulnerable to corruption. This flow of revenue into an already opaque sector is at risk of not being included in financial plans or budgets and could go entirely unreported, resulting in monies being used as slush-funds for secretive and unregulated military activity and procurement. Examples of confidential income includes revenues from UN peacekeeping missions, natural resources extraction, national arms industries, and military-owned enterprises (See Figure 4).

Figure 4: Disclosure of defence income vis-a-vis military-owned enterprises, GDI

| Countries with defence institutions that have commercial enterprises constituting 1%-10% of the defence budget. | Extent of defence income that is made public | Countries with defence institutions that have commercial businesses that are major enterprises or constitute more than 10% of the defence budget.[20] |
|---|---|---|
| United Kingdom, Portugal | There is **full publication** of all sources of income, the amounts received, and the allocation of this income. | Georgia, Malaysia |
| Argentina, Hungary, Serbia | There is full publication of all sources of income, the amounts received, but **inadequate information on the allocation of income**. | Switzerland, Ukraine |
| Armenia, Chile, Colombia, Kenya, Uganda | There is full publication of income sources, but there may be **little or no release of information about amounts received or the allocation of this income**, or there may be full publication but only of **selected income sources**. | |
| Albania, Canada, Lebanon, Mexico, Montenegro | There is only **selective publication** of income sources, and no information released on amounts received or the allocation of this income. | Ghana, India, Iran, Tanzania |
| Cote d'Ivoire, Mali, Nigeria, Saudi Arabia, Thailand, Turkey | There is **no publication** of noncentral government sources of funding, or the information that is published is considered unreliable. | Algeria, Angola, Burkina Faso, Cameroon, Egypt, Ghana, Iraq, Jordan, Malaysia, Myanmar, Oman, Qatar, South Sudan, Sudan, Venezuela, Vietnam, Zimbabwe |

**Asset disposal** is another potential income stream that is vulnerable to corruption. It can occur through the misappropriation or sale of property portfolios and surplus equipment. Even large assets can be poorly controlled and easy to sell off corruptly or undervalued. These risks are particularly pronounced in nations that are selling or disposing of large quantities of assets, or in fragile and post-conflict environments where assets cannot be well protected.[21]

In countries with well-managed asset disposal processes, open tendering is common for non-strategic assets such as real estate and movable property. It is also common for income to be reflected in the budget, but for asset disposals, the origin or nature of the income may not be clear. There may be a specialised institution created for the purpose of handling asset disposals for the public sector, or disposals may be handled by the Ministry of Finance or Economic Development, both of which limit the influence of the Ministry of Defence over the asset disposal process. These limitations also make it more challenging to identify which assets originated from the defence sector. Results are often aggregated and distributed across various publication outlets, making it difficult to understand what was sold, to whom, for how much, and where the proceeds were directed.

20 Other countries that are likely to have enterprises generating more than 10% of the budget, but for which there is insufficient information publicly available to assess: Bangladesh, China, Indonesia, and Russia.

21 Transparency International, Defence & Security, "Building Integrity and Countering Corruption in Defence & Security: 20 Practical Reforms" (London: Transparency International UK, 2011), 69.

In resource-poor or conflict-affected countries, a major issue is the lack of well-maintained asset registers, which obscure the defence sector's existing property. Combined with a failure to release information about planned disposals, which happens in over a third of countries in the GDI, there is little opportunity to track the disposal process. In fact, 40 per cent of countries score 0 here, meaning no information is released about the disposal process. Similarly, transparency around the financial results of disposals is extremely poor. For close to half of the index, there is no public knowledge about the financial results of the disposal process.[22]

### Box 8: Types of defence assets marked for disposal

**Asset Disposal:** The process of selling, auctioning or otherwise disposing of military assets, which can include:

**Single Use Military Equipment (SUME):** military equipment which cannot be used for civilian purposes. This includes weapons as well as equipment which supports and delivers them, e.g. warships, submarines, fighter aircraft, tanks, missiles and launchers.

**Land and Buildings:** offices, warehouses, hospitals, barracks, hangars, runways, car parks and associated holdings (excluding dwellings).

**Assets under construction.**

**Transport equipment:** any equipment that moves either people or objects, e.g. lorries, trains, ambulances and aircraft.

**Plant and Machinery:** portable and fixed equipment needed either to repair or maintain assets or for administrative purposes.

**Information Technology (IT) and Communications:** All IT systems and the respective hardware and software.

## Defence Procurement

Defence procurement is considered one of the most sensitive and secretive areas of military spending, even though the majority of purchases are ordinary goods and technology, rather than arms, components, and ammunitions. Given the size of defence budgets and opacity with which much military procurement is conducted, procurement is highly susceptible to corruption. Ineffective or non-existent procurement processes do not just lead to waste and corruption, they also result in purchases with high costs and questionable strategic purpose, as well as delays and cost overruns.[23]

Enhancing transparency and access to information on the entire procurement cycle can significantly reduce corruption risk, facilitating scrutiny by oversight institutions, increasing external involvement in the procurement planning process, and mitigating opportunities for corruption at key junctures of the process. However, given the sensitivities attached to the procurement of goods that can impact national security, efforts to enhance defence procurement transparency have had limited success (See Figure 5).

### Box 9: Good practice in defence procurement transparency

**Good practice in defence procurement transparency involves the following:**

For both confidential and non-confidential purchases, there is a disclosure of the tender and the contract award.

For the contract, there is a description of the item purchased, the winning bidder, the beneficial owners, price paid, whole of lifecycle costs, cost of servicing, costs of parts, and delivery/ completion date.

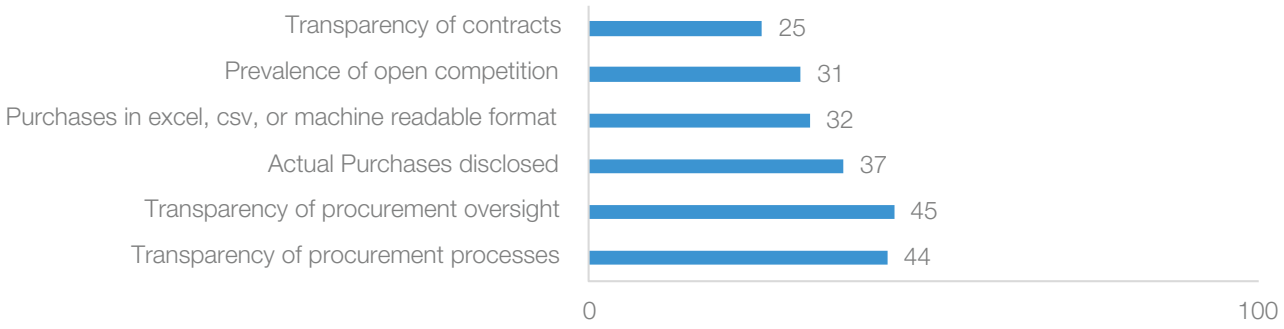
All postaward modifications are made available, such as change of sub-contractor, change of beneficial owner, and additional costs, such as consultants.

Very little data from the tender/ contract is redacted for national security reasons.

22 Beyond the financial results, there is also a dearth of information about recycling, redistribution, donations, abandonment, and destruction of assets, which is an issue in most of the countries in the index.

23 Perlo-Freeman, "Transparency and accountability in military spending." SIPRI, August 2016.

**Figure 5: Access to defence procurement data, average scores across the GDI**




Most national public procurement legislation contains defence-related exemptions, which can be so broad as to exempt the vast majority of defence procurement from standard procedures, even for non-sensitive goods and equipment. In fact, defence procurement legislation is either non-existent or completely ineffective at regulating the majority of defence acquisitions in nearly 40% of countries in the GDI. Many planned defence purchases are assigned restricted information categories (see discussion on secrecy classification above) that hampers efforts to determine spending allocation. Confidential purchases are then legally exempted from procurement laws.

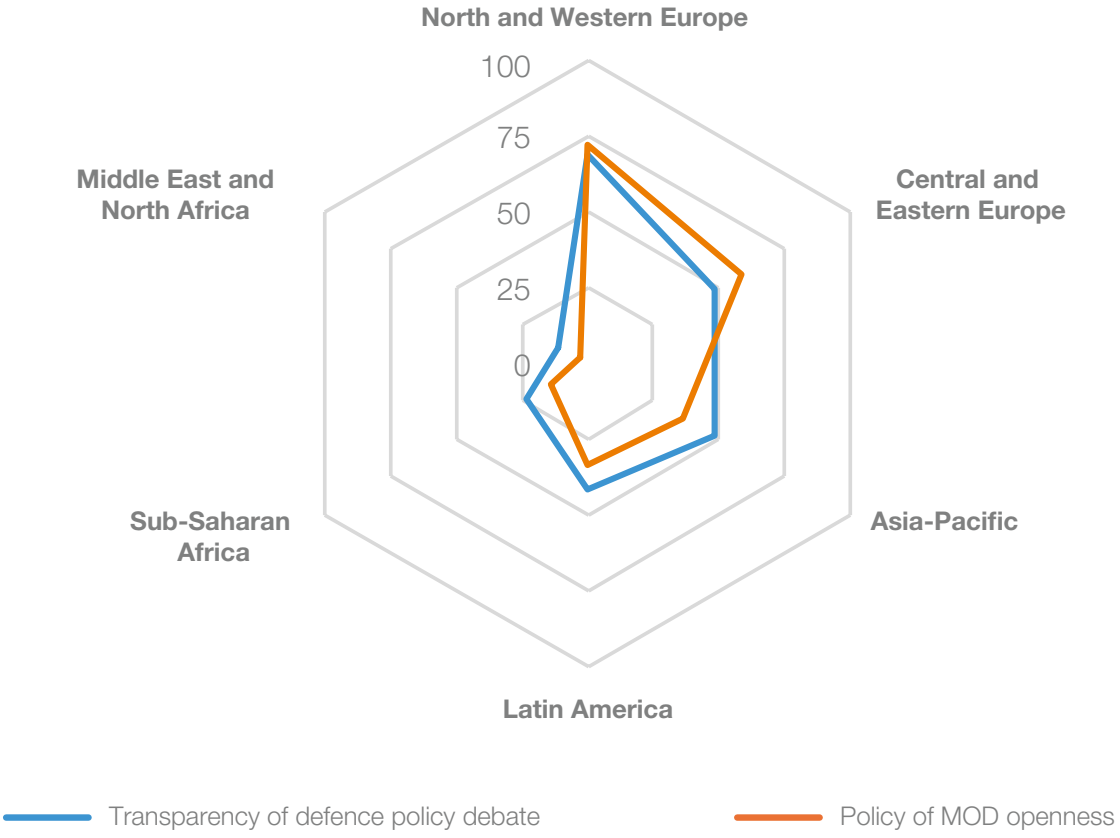
Information on defence procurement often filters down to media and civil society well after the purchase, in some cases as late as the following year's defence budget. Many of the countries in the GDI fail to release details on the defence contracts awarded through procurement processes, and even in those countries that do release contract data, information on post-award modifications is rarely available (See Figure 6 for details on NATO countries).

**Figure 6: Defence procurement transparency in NATO countries**

| | Transparency of procurement processes | Transparency of procurement oversight activity | Actual purchases disclosed | Transparency of contracts (including post-award modifications) |
|---|---|---|---|---|
| **Score: 100 Very Robust** | Sweden, United Kingdom, United States, Belgium, Estonia | Belgium, Estonia, Finland, Italy, Lithuania, Netherlands, Norway, Sweden, United Kingdom | Canada | Belgium, Latvia |
| **Score: 75 Robust** | Albania, Finland, France, Italy, Latvia, Norway, Portugal, | Albania, Denmark, Germany, Latvia, Montenegro, North Macedonia, Portugal, United States | Belgium, Estonia, Finland, Greece, Italy, Latvia, Netherlands, North Macedonia, Norway, Poland, Portugal, United States | Finland, North Macedonia |
| **Score: 50 Moderate** | Canada, Germany, Greece, Hungary, Lithuania, Netherlands, North Macedonia, Poland, Spain | Canada, France, Greece, Spain | Albania, Germany, Spain, Sweden, United Kingdom | Canada, Estonia, Germany, Greece, Italy, Lithuania, Montenegro, Netherlands, Norway, United Kingdom, United States |
| **Score: 25 Weak** | Denmark, Turkey | | Denmark, France, Hungary, Lithuania, Montenegro, Turkey | Albania, Denmark, France, Hungary, Spain, Sweden, Turkey |
| **Score: 0 None** | Montenegro | Hungary, Poland, Turkey | | Poland, Portugal |

An encouraging sign with regards to defence procurement is the impact of e-procurement initiatives across the whole of government. In countries with well-defined secrecy classification practices that support the right to information, most non-strategic goods are procured through open tendering. Still, nearly 60% of countries fail to release defence procurement data in machine-readable format, such as excel or csv.

**Figure 7: Access to defence institutions, regional averages**




## Transparency for Civic Engagement in Defence Matters

Civil society can play a key role in in the development of policy by lobbying for changes and by contributing to citizen oversight of the government's work and mandate. Among other activities, this can include monitoring how public services, such as defence and security, are delivered, and how human rights are both violated and upheld by government actors.[24] In relation to the defence sector in particular, civic space and civil society engagement are crucial to strengthening the defence governance chain; from communicating public opinions during defence policy formulation, to supporting and monitoring the execution of budgets and procurement processes, to holding government to account for actions that may not serve the national or public interest.

However, engagement between civil society and defence institutions in many countries is often limited due to traditions of secrecy, the prioritisation of national security concerns over civil liberties, the technical nature of the defence sector, and the lack of trust between civil society and defence institutions. In the current global context marked by shrinking civic space,[25] particularly post-pandemic, it is more important than ever to ensure civil society have information they need to fully understand their government's priorities and the freedom to voice their concerns and bring their expertise to the table.[26]

The strength of civil society engagement in defence issues goes hand-in-hand with the *government's openness* to engagement (See Figure 7). If this is limited, then the quality of dialogue on policy and strategic issues, and the effectiveness of participatory mechanisms, are also likely to be limited, as the

24 DCAF, "Civil Society Involvement in Security Sector Reform and Governance," Tool 6 (Geneva Centre for Security Sector Governance (DCAF), 2015), 3.

25 Saskia Brechenmacher and Thomas Carothers, "Defending Civic Space: Is the International Community Stuck?" (Washington, D.C.: Carnegie Endowment for International Peace, October 22, 2019).

26 Colin Anderson et al., "Navigating Civic Space in a Time of Covid: Synthesis Report" (Brighton: Institute of Development Studies, May 2021).

government and defence institutions can easily withdraw from these processes. GDI data reveals that regardless of regional or income grouping, general public debate on defence issues is always more frequent than specific strategic or policy discussions. When the latter occur, the executive is rarely involved, and dialogue is confined to the media and civil society. This dilutes the potential impact of these debates.

As such, civil society can find themselves treading carefully between wanting to engage fully and frankly on defence issues, and not wanting to be shut out completely by defence actors – or worse, become targets for harassment and intimidation.

A critical factor in robust civic engagement in defence matters is the transparency of planning processes, specifically *before* actions are taken. In addition to budgetary and procurement information, the disclosure of information during the planning processes for defence purchases and asset disposals ensures that civil society can engage meaningfully with defence institutions during both peacetime and post-conflict situations, and can be prepared for conflict scenarios as they arise.

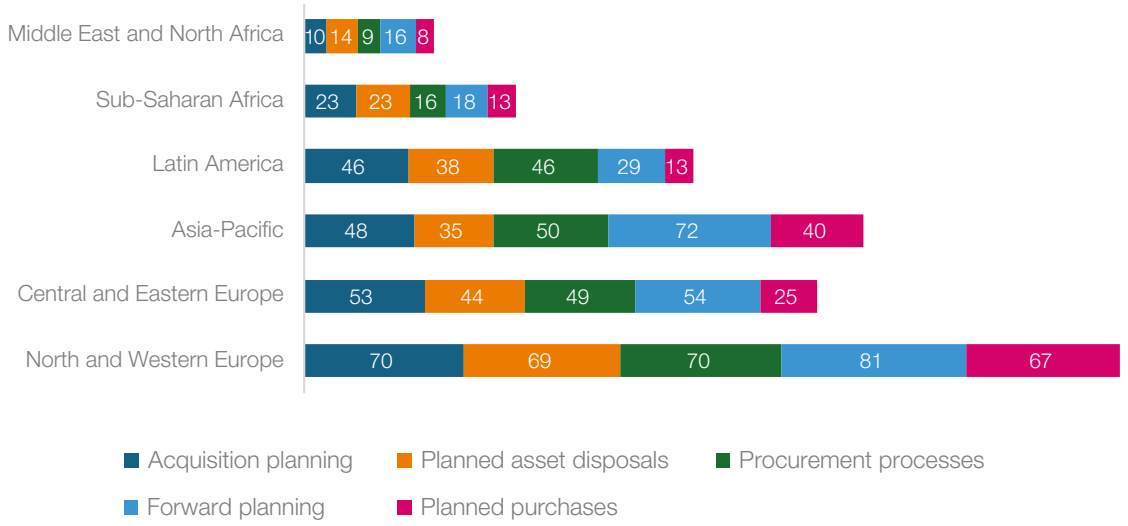
Unfortunately, only a quarter of countries in the GDI have a clear process in place for the entire defence acquisition planning cycle, where connections between specific purchases and the defence strategy are made explicit. Less than 10 per cent of countries provide information about the entire planning process, whilst in half the countries in the index there is extremely limited or no transparency at all (See Figure 8).

**Box 10: Good practice in defence purchase planning**

**Good practice in defence purchase planning includes the following:**

- The government publishes comprehensive forward planning for potential purchases which extends 10-15 years in advance, e.g. through a strategic defence review, white paper or similar.
- The government publishes the plans for defence purchases in detail for at least the next 4 years.
- The adequate and timely information (e.g. elements of the defence equipment plan, itemized budget proposals) is sufficient to enable prospective suppliers to prepare and seek further information.
- Information is also sufficient for oversight agencies and civil society to debate the necessity of the proposed purchases (e.g. the average procurement duration, justification of exceptions, and specific overview records by type of bidding procedure).

**Figure 8: Disclosure of information on defence planning and processes: Regional averages**

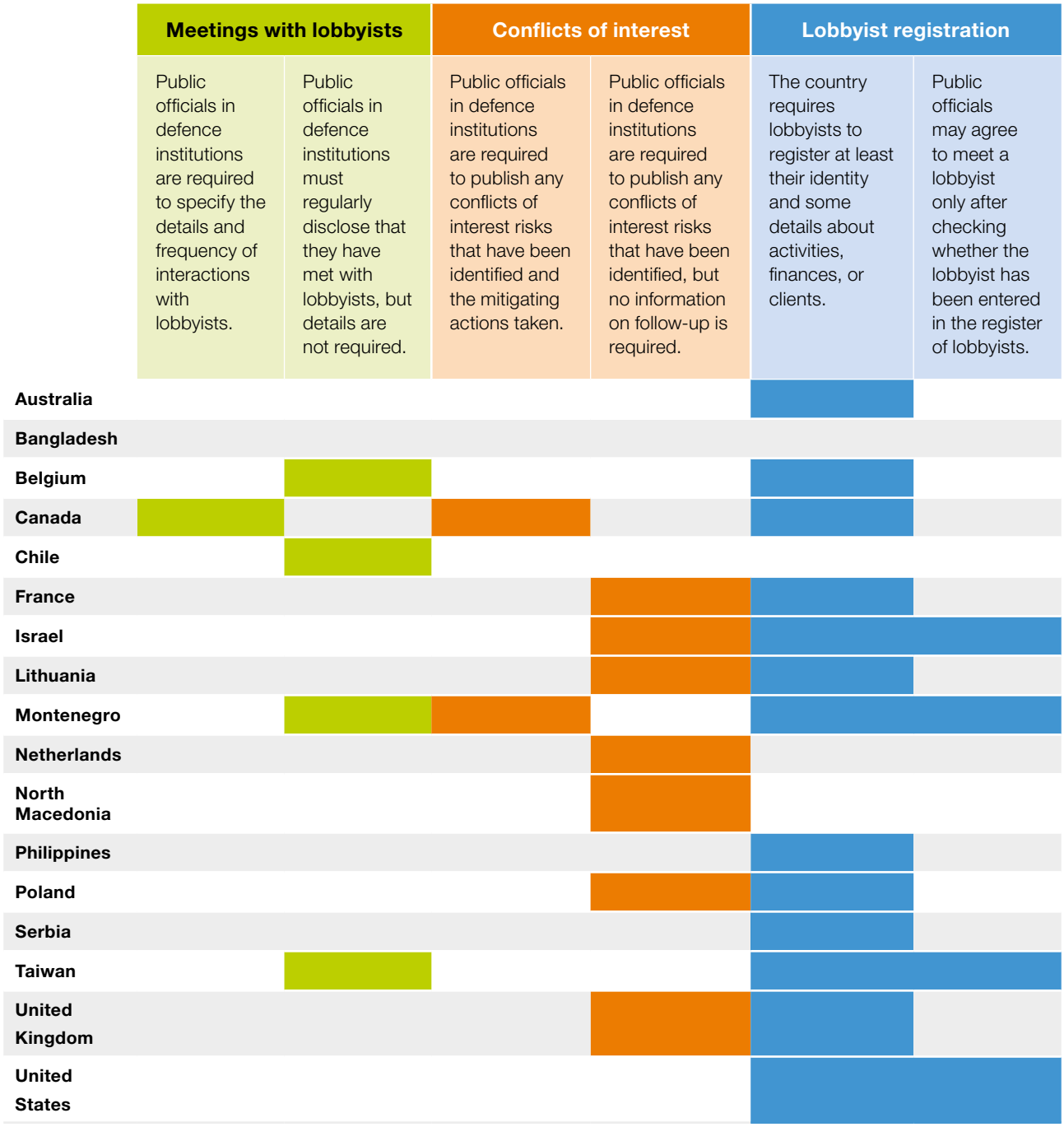



The speed with which states are developing and implementing new technologies, including advanced weapons systems, AI-enabled hardware and communications technology, will further strain standard procurement planning processes and considerably increase the risk that such acquisitions may be unplanned and opportunistic. Transparency around defence purchase planning can safeguard against government "silos" and opportunistic acquisitions that exclude valuable contributions from external actors.

The combination of poor transparency, lack of public debate, and the highly technical nature of complex new technologies increases corruption risks associated with undue influence from the defence industry. Private sector actors hold a significantly greater amount of knowledge and expertise on these products than governments. Industry influence can be exerted over governments through financial means, be they political contributions or direct financial interests of decision-makers that can generate conflicts of interest. Pathways of influence facilitate the transfer of information between the public and private sector through lobbying and the outsourcing of expertise to private consultancies. It is rare for lobbying in the defence sector to be regulated, and even when legal frameworks are in place, they do not capture the true extent of the influencing (See Figure 9).

Military Helicopter (Photo Credit: onkelglocke, Pixabay)

**Figure 9: Transparency of Defence Lobbying in countries that regulate lobbying**[27]




Given the sophisticated technical expertise required and the short procurement timelines, the defence industry stands to gain even more influence over defence policy and procurement as governments increasingly outsource decisions to the private contractors leading in the development of new technologies. The lack of transparency around lobbying is a major corruption vulnerability,[28] as undue influence from the private sector in both policymaking and procurement has been found to increase corruption risks and conflict of interests in countries with powerful defence industry players.[29]

27 Almost 80 percent of countries in the GDI do not regulate lobbying in the defence sector.

28 Transparency International UK, "Understanding Access and Potential Influence in Westminster" (London: Transparency International UK, October 2021).

29 Transparency International, Defence & Security, "Defence Industry Influence on European Policy Agendas." Transparency International, 2021.

# SECTION 2: CASE STUDIES

# ARMENIA: ACCESS TO INFORMATION IN THE DEFENCE SECTOR

## Overview

1. Armenia has seen high levels of defence spending because of its decades-long conflict with Azerbaijan over the Nagorno-Karabakh territory, which has recently concluded with major losses for Armenia.
2. Access to information is enshrined in a national freedom of information law, but has been curtailed severely by the 2024 states secrets law, which prohibits the release of information related to most defence spending.
3. There are no balancing tests specified in the law requiring officials to determine harm of disclosure or benefit to the public interest, nor an independent oversight body to assist with implementation or clarification of legal rules.
4. The confidentiality of information can be renewed every five years, allowing for permanent classification of secrecy and thus indefinitely withheld from disclosure.
5. A Civic Oversight Platform for defence and security matters was created in 2020 with the support of the OSCE, together with the National Assembly Standing Committee on Defence and Security and the National Security Council, but focused exclusively on internal police reforms. As of 2024 it is still not functional.

## Country Context

Freedom of information was established in Armenia in 2003 with the enactment of the Law on Freedom of Information, which has upheld access to information reasonably well over the past two decades. However, the past years have seen extensive efforts to reform the access to information framework, as well as the framework surrounding work in the defence sector. In January 2024 a new law on state secrets came into force that severely limits access to information related to national security, particularly defence procurement and defence production. This was preceded by amendments in 2022 assigning full control and oversight of defence procurement to the Ministry of Defence. In addition, discussions are underway to reform access to public information, including a draft law on proactively provided information, which many civil society organisations have found to be regressive and unclear.[30]

Against this background, the Armenian armed forces have been involved in several high-profile corruption scandals over defence procurement. Former Defence Minister David Tonoyan was arrested in September 2021 and charged with fraud and embezzlement of nearly USD6m.[31] Charges were also brought against the former head and deputy head of the General Directorate of the armed forces, the head of the aviation technical property service, and its chief engineer.[32] The former deputy chief of the

30 *CSO Meter*. "Armenia: Draft Law on Access to Information Criticised by CSOs." January 30, 2024.

31 Khulian, Artak, and Naira Nalbandian. "Former Armenian Defense Minister Arrested." «Ազատ Եվրոպա/Ազատություն» ռադիոկայան, September 30, 2021.

32 https://www.rferl.org/a/armania-military-weapons-fraud/31662118.html, https://factor.am/en/4898.html, https://168.am/2021/11/02/1601332.html, https://fip.am/en/35591

Monastery Valley, Armenia (Photo Credit:Ivars Utināns, Unsplash)

Armenian military's General Staff, Stepan Galstyan, was arrested in October 2021 as part of a criminal case into purchases of allegedly faulty weapons and ammunitions that involved also former Defense Minister David Tonoyan and arms dealer David Galstyan[33].

Defence procurement has been a priority for the Armenian government for many decades, due to its ongoing conflict with Azerbaijan, which escalated in 1991-1994, 2020, and 2023. As of the end of 2023, the disputed area, with a high percentage of ethnic Armenian population, is officially under the control of Azerbaijan. Since then, Armenia has suffered heavy casualties, loss of equipment, and the expulsion of its troops followed by the exodus of ethnic Armenians from the territory.

## RTI law and classification

Much work has been done to establish and strengthen the access to information framework in Armenia, however recent legal developments place public access to defence-related information in jeopardy. The new law also places extraordinary limits on release of information pertaining to defence purchases, armaments and equipment, production capacities, and even defence suppliers. (See table below). Civil society organisations have expressed concerns over the new Law on State Secrets (2024)—particularly about language outlining "limited distribution," which gives wide discretion to government officials to refuse disclosure of information indefinitely–and have called for a better-defined classification system, as well as the establishment of an independent appeals body that can adjudicate claims over denials of information requests.

33 Mejlumyan, Ani. "Armenian Ex-Defense Minister Arrested for Embezzlement and Faulty Weapons Purchases." *Eurasianet*, September 30, 2021. https://fip.am/en/35591

Table 1: Key features of ATI legal frameworks - Armenia

| | |
|---|---|
| **National legislation.** Any restriction on right to information must be present in the applicable national legislation | Law of the Republic of Armenia on Freedom of Information (2003)<br>Law on State Secrets (2024) |
| **Exceptions related to defence.** The exceptions to the right of access based on national security are well-defined and consistent with international standards. | Art 8 of the Law on State Secrets prescribes as a state secret/ classified information, inter alia, any information about the volumes of state defense orders, programs, the production, repair, supplies of armaments and military equipment, the availability and development of their production capacities, the mutual cooperation ties established between organisations for this purpose, the producers of the mentioned armaments and military equipment or those performing technical and scientific developments.<br>According to the Art 29 of the same law, government officials can assign "limited distribution" to any information for a certain period of time in defense of the state, ensuring national security, as well as protection of foreign relations, political and economic interests. This is ostensibly based on official necessity, and is not subject to publication during the entire period of limitation. |
| **Harm test.** Information may be exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm | None. Based on absolute exceptions rather than a specific harm. |
| **Public Interest Test.** The law should provide for a public interest test when classified information is requested | Only in a general sense: if the decline of the information request will have a negative influence on the implementation of state programs of the Republic of Armenia directed to socio-economic, scientific, spiritual and cultural development. |
| **Appeals.** Requesters have the right to lodge an appeal with an independent administrative oversight body. | Appeals may be filed with the Ombudsman, however, requesters must rely on the court system to compel disclosure in the face of administrative denials, which can be expensive and lengthy. |
| **Declassification.** There should be a maximum expiry time in every secrecy regime | None. Confidentiality can be renewed every five years, allowing for permanent classification. |

**The new law places extraordinary limits on release of information pertaining to defence purchases, armaments and equipment, production capacities, and even defence suppliers.**

# Defence Finances

The defence budget comprises an integral part of the general budget and undergoes the same procedure as the general budget. Key items are openly accessible in each year's approved budget, though with a general outline. There is information on expenditures on military R&D and social support to the families of the deceased servicemen. Besides than that the information on expenditure is vague, in contrast to budgetary information for other ministries across government (See Table below). The lack of information provided for defence makes it difficult or impossible to exercise oversight of the defence budget.

Some sources of income from outside the central budget are made transparent through regulations. There are separate accounts in the Treasury for financial proceeds accumulated by the medical institutions under the auspices of the Ministry of Defence, and another account for the initiative by the MoD to establish an Insurance Foundation for Servicemen. However, the use of off-balance resources by the MoD is deemed confidential by the Audit Court and information is not released on this topic.

Defence allocations are published in the Law on the Budget of the specific year. However, the non-classified part of the budget allocated for military needs in practice contains excessive and unnecessary details. In 2020, the expenditure report was comprised of 2,190 lines and included items such as printing services (ca. AMD106 or USD equivalent). Such level of detail obscures the larger volumes of spending and complicates actual oversight, which does not increase transparency and accountability.

**Table 2: Open Budget Index scores among ATI case studies, International Budget Partnership 2023**

| Country | Transparency Score (out of 100) | Rank (out of 125 countries) | % change since last index[34] |
|---|---|---|---|
| **Moldova** | 81 | 5 | 25% |
| **Bulgaria** | 79 | 10 | 11% |
| **Slovakia** | 69 | 21 | 6% |
| **Croatia** | 67 | 24 | 5% |
| **Armenia** | 60 | 41 | 2% |

**Table 3: Military expenditures among ATI case studies, SIPRI 2023[35]**

| Country | Military spending (USD millions) | % change 2022-2023 | % change 2014-2023 | Per capita spending | % of government spending |
|---|---|---|---|---|---|
| **Azerbaijan** | 3561.7 | 19% | 4% | 342.0 | 14.71% |
| **Belarus** | 1403.1 | 27% | 71% | 147.7 | 50.59% |
| **Georgia** | 504.6 | 40% | 21% | 135.4 | 5.54% |
| **Moldova** | 93.4 | 96% | 239% | 27.2 | 1.40% |
| **Armenia** | 1329.5 | 67% | 190% | 478.6 | 19.96% |

34 The +/- indicates whether the Transparency Score rose or fell against the last iteration of the Open Budget Index.

35 Average % of government spending: Eastern Europe: 23.79% (Ukraine is highest at 58.17%); Central Europe: 4.82% (Poland is highest at 8.12%)

**Understanding Armenia's sharp increase in military spending through a post-conflict lens:**

### Why is there such an urgent new focus on building up defence?

Armenia experienced significant military losses over the past few years: major losses of contested territory in the 2020 Nagorno-Karabakh War with Azerbaijan, subsequent bouts of fighting, a significant number of casualties and losses of own territories in 2021 and 2022, as well as exodus of the Armenian population from Nagorno Karabakh in 2023. The border with Azerbaijan changed and extended, which needs a new fortification system because of ongoing war rhetoric from Azerbaijan, occuring in the midst of internationally-broked peace negotiations. Traditionally, Armenia has received military protection from Russia and was a member of the Collective Security Treaty Organization (CSTO). However, recent military escalations have resulted in the failure of both Russia and the CSTO to implement partnership commitments in defence of Armenia.

As a result, there has been a concerted effort by Armenia to build up its own military capacities with new partnerships.

### Where is the dramatic increase in public funds coming from?

The mass immigration of Russian nationals to Armenia and the boom in business arising from this influx can account for the unprecedented economic capacity of Armenia in 2023. The net profit of the banks in 2022 turned out to be the highest in the history of independent Armenia, which is three times more than the indicators of the previous year. In January 2023, the net inflow of cash receipts into Armenia increased more than 13 times the previous year.[36]

## Defence Procurement

All defence purchases, except those classified as confidential and secret, are publicly accessible through ARMEPS (www.armeps.am), the Armenian Electronic Procurement System, together with the list of the purchases and the contracts concluded with suppliers. Data is released in an Excel spreadsheet through the electronic procurement system, but the data lacks confidential information on arms procurement and related items, and with the new states secret law, the scope of data that may be withheld is much broader. Historically, information on classified procurement is exposed long after the purchase - through the complaints system, statements of law enforcement institutions wherever there was criminal prosecution in place, court litigation materials, as well as in the reports of international organisations and experts and media coverage. This fragmentary information is insufficient for a thorough analysis of procurement processes.

In July 2022 a new amendment to the Law on Defence (ՀՕ-334-Ն, adopted on 7 July 2022) entered into force giving the Ministry of Defence full control and oversight of procurement issues within the Ministry.

The amendment allows the Ministry to conduct purchasing with little involvement of the National Assembly. This includes carrying out purchases of weapons and military equipment, food, goods and other property and material resources for the needs of the armed forces, managing the barracks fund of the armed forces, and supervising the expenditure of financial resources and logistics by the armed forces and other bodies of the defence sector.

Classification of a significant scope of data compromises the quality of oversight by internal and external institutions. Internal control reports are not publicly available and oversight by the Chamber of Audit is not transparent. For example, there is information about two sessions in 2018 and 2019 that mentioned the plans to conduct an audit in the defence sector, however there is no data provided about this in the 2018 and 2019 annual reports. There is information about the oversight of procurement, generation and spending of extrabudgetary funds, however it does not correspond with any particular reports. While other sectors can be controlled through public oversight, classification of a large volume of defence procurement leaves the sector out of the range of accountability.

36 Freund, Josephine. "Armenia's New National Budget: A Drastic New Commitment to Military Capacity." *Caspian Policy Center*, March 9, 2023.

# Transparency for Civic Engagement in defence matters

**Table 4: Access to key documents related to defence matters - Armenia**

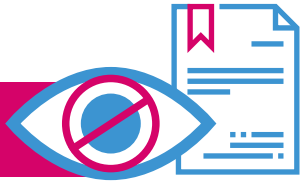
| Information | Public availability | Additional explanation |
|---|---|---|
| **Defence Strategy/ Policy** | The National Security Strategy is publicly available. | The public can access information on proposed law drafts and initiatives through a common portal, which includes matters of defence and security. |
| **Audit reports** | The Audit Chamber's annual reports and conclusions are published on the official website of the Audit Chamber and website. | Audit Chamber reports are publicly available except for the information that is classified as secret. |
| **Asset Disposals** | Information about the tender, auction or direct sale and the details about the relevant assets can be found on State Property Management Department official website; however, there is no information about the signed contracts and financial results of asset disposals. | Announcements on the disposal of the significant assets are not available. |

The Ministry of Defence provides a comprehensive Concept on Public Awareness, stressing the importance and outlining the scope of public consultations and cooperation with media and CSOs. The main purpose of the approach is to define the ways and means of creating public awareness strategy on the activities of the MoD and the General Staff of the Armed Forces and to increase the level of public awareness on the programs and reforms which are designed to improve and modernize the defence sector.

However, consultations over defence matters in Armenia are rare. A Civic Oversight Platform for defence and security matters was created in 2020 with the support of the OSCE, together with the National Assembly Standing Committee on Defence and Security and the National Security Council. Most discussions focused on internal matters, such as police reforms, rather than defence sector policies, and activity declined drastically after a few follow-on activities. There is also little debate in parliament, given regular boycotts of the opposition, and serious tensions between the parliamentary factions.

INTERNAL CONTROL REPORTS ARE

**NOT PUBLICLY AVAILABLE**



AND OVERSIGHT BY THE CHAMBER OF AUDIT IS **NOT TRANSPARENT**

Republic square, Armenia (Photo Credit: Maluku, Pixabay)

## Recommendations

1. Advocate for the reform of the **access to information law** so that harm and public interest tests are used to determine whether information should be withheld from disclosure, rather than relying on absolute definitions as specified in the new states secret law. The access to information law should also override any other law addressing information access, including the states secret law.[37]

2. Advocate for the reform of the **states secret law**, particularly to remove the absolute definition of secret/classified information, and to adhere to the Tshwane Principles.[38] Because of the specificity of the law, it is unlikely that government institutions will release any defence-related information without legal reforms. It is also advisable to eliminate or revise the category of "limited distribution," and to establish a maximum expiry time for classified information.

3. Continue advocating for the establishment of an independent appeals/oversight body for freedom of information. At the minimum, this body should have the mandate to issue decisions that clarify the scope of relevant laws and to identify weaknesses in the implementation of access to information. Ideally, the body should have the authority to compel disclosure and conduct investigations.

4. Advocate for renewed operation of the Civic Oversight Platform for defence and security matters, which would allow civil society actors to provide input into national defence discussions, defence strategy developments, and implementing policies.

37 See the advocacy guide published by TI-DS in 2024 for an in-depth review of tactics and approaches to establishing access to information in the defence sector: Transparency International Defence & Security. "Defending Transparency: An Advocate's Guide to Counteracting Defence Corruption." London, 2024. https://ti-defence.org/publications/defence-security-sector-advocacy-toolkit-guide/.

38 Further clarifying existing terms of the law may unintentionally reinforce their current legal interpretations and absolute definition of secret/classified information, so it is advisable to avoid this approach and instead advocate for improved categories that align more closely with the Tshwane Principles.

CASE STUDY

# GUATEMALA: ACCESS TO INFORMATION IN THE DEFENCE SECTOR

## Overview

1. Guatemala has endured a growing corruption crisis for the past decade, as the presidency and the powerful Public Prosecutor's office have stifled anti-corruption efforts, forced anti-corruption officials into exile, and blocked potential reform candidates from elections. Because the Secretariat for Access to Public Information (SECAI) is required to work with the prosecutor's office on ATI enforcement, this has stymied implementation of the law.

2. There is a strong access to information law with limited exceptions and clear balancing tests (harm and public interest) to determine disclosure of information. By defining national security and balancing these tests, the Guatemalan law ensures that classification is an exception rather than a rule. However, a significant challenges lies in the lack of enforcement mechanisms when institutional bodies deny access to information. The SECAI and the Ombudsman's Office have limited authority to enforce the Law on Access to Public Information (LAIP) and can only offer petitioners non-binding appeals processes in cases of denials.

3. Efforts by the independent appeals body (SECAI) to enforce adherence to the law have been thwarted by the government[39] in the past decade, despite its initial success in establishing access to information systems in the public sector.

4. Defence finances and defence procurement are transparent and accessible, with online transparency portals and e-procurement services. The Ministry of Finance publishes the approved budgets for the fiscal year on its website, and there is also a Budget Transparency Portal that provides citizen documents and the budget in open data format. While there are few official consultation processes on defence matters, inter-institutional collaboration on defence is well-established, and access to policy documents is extensive.

## Country Context

Access to information in Guatemala is established in the legal framework by the 2008 Ley de Acceso a la Información Pública (Law on Access to Public Information or LAIP), and Article 30 of the Constitution. Since 2008, transparency has been embedded within the public administration through the extensive work of the Secretariat for Access to Public Information (SECAI), under the auspices of the Human Rights Ombudsman (PDH). However, there have been a series of events over the past few years that have adversely affected the ability of these institutions to protect access to information within the public sector. Because SECAI is required to collaborate with the Public Prosecutor's office in order to sanction institutions for violating the provisions of LAIP, enforcement has become nearly impossible since Consuelo Porras took office. Since 2018, she has consistently shut down corruption cases and been sanctioned by the US government twice for

39 Government here refers to the previous administrations led by Jimmy Morales (2016-2020) and Alejandro Giammatei (2020-2024).

THE **"NGO LAW" WAS PASSED IN 2020**, AND UPHELD BY THE CONSTITUTIONAL COURT IN 2021, **FORCING NON-GOVERNMENTAL ORGANISATIONS** (NGOS) TO:

**REGISTER WITH THE GOVERNMENT**

**REPORT THEIR DONATIONS**

**ALLOW THEIR ACCOUNTS TO BE INSPECTED BY THE GOVERNMENT**


undermining democracy.[40] In 2019, the UN-supported International Commission against Impunity in Guatemala (CICIG) was abolished by the president, Jimmy Morales, who was also under investigation for corruption and election financing violations.[41]

A controversial "NGO law" was passed in 2020, and upheld by the Constitutional Court in 2021, forcing Non-Governmental Organisations (NGOs) to register with the government, report their donations, and allow their accounts to be inspected by the government. Under certain circumstances, the law also allows government entities to dissolve, control, and monitor NGOs.[42] According to media rights advocates, the Giammatei government has attempted to limit freedom of expression through spurious lawsuits, subpoenas, telephone confiscations, and the execution of search warrants and home searches of media members and justice defenders.[43]

The activity of "netcenters"—collections of social media accounts organised to appear as independent individual users but in fact centrally controlled and used to manipulate discussions, spread misinformation, and threaten people on the internet—has also increased over the last decade.[44] Netcenters create fake social media accounts to criticize and defame journalists, judges, prosecutors, and citizens who report on corruption.

Under the administrations of Jimmy Morales (2016-2020) and Alejandro Giammetti (2020-2024), a number of high-profile anti-corruption officials have either been arrested or gone into exile, media organisations have been shut down, journalists have been jailed or forced to flee the country, and existing transparency initiatives within government have been stymied.[45] With the election of a new president in June 2023, it remains to be seen whether anticorruption and transparency efforts can be resuscitated in the midst of severe democratic backsliding. [46]

The new administration, led by Bernardo Arévalo, started in January 2024. Arévalo, whose political campaign centered on an anti-corruption platform, took office with an important support from indigenous groups and the international community.[47] Since the start of this administration, the Presidential Commission on Open and Electronic Government has been reactivated. He also recently established a National Commission against Corruption (CNC) within the Executive Branch, along with the Integrity Network (Red de Integridad) to strengthen transparency and accountability in government.

## RTI law and classification

Guatemala's access to information law and corresponding implementing actions established a strong framework for providing information about the public sector to the public (see table below). Although most government agencies have responsibility for access to information, public institutions across government regularly fail to comply with the law since SECAI lost its mandate to sanction for violations. Government data portals ceased to function, and the public procurement portal was hacked and place offline for months.

40 Perez Diaz, Sonia. "Why Is the Guatemala Attorney General Going after the New President?" *AP News*, January 17, 2024, sec. World News.

41 Washington Office on Latin America (WOLA). "Fact Sheet: The CICIG's Legacy in Fighting Corruption in Guatemala," August 27, 2019.

42 Volet, Charlotte, and Laurence Ouellet-Boivin. "Shrinking Democratic Space for Civil Society in Guatemala - Alternatives Humanitaires." *Alternatives Humanitaires*, November 20, 2023, sec. Central America: a forgotten subcontinent?; Menchu, Sofia. "Guatemala's Top Court Backs Controversial NGO Law, Overturns Past Ruling." *Reuters*, May 13, 2021, sec. Americas.

43 "2023 Human Rights Report: Guatemala." Washington, DC: U.S. Department of State, 2024.

44 "Report: "Bots, Netcenters and the Fight against Impunity." International Commission against Impunity in Guatemala (CICIG), May 20, 2019.

45 Blitzer, Jonathan. "The Exile of Guatemala's Anti-Corruption Efforts." *The New Yorker*, April 29, 2022; "Guatemala: No Press Freedom, No Democracy." Washington, DC: Freedom House, May 17, 2023; Kahn, Gretel. "Meet the Journalists Defying a Widening Crackdown on Press Freedom in Guatemala." Oxford: Reuters Institute for the Study of Journalism, May 25, 2023.

46 Perez Diaz, Sonia. "Guatemalan President Bernardo Arévalo Says He Found a 'semi-Destroyed Country' on Taking Office." *AP News*, June 20, 2024, World News edition.

47 Washington Office on Latin America (WOLA. "Ushering in a New Period: Bernardo Arévalo's Opportunities and Challenges to Restoring Democracy in Guatemala," January 9, 2024.

**Table 5: Key features of ATI legal frameworks- Guatemala**

| | |
|---|---|
| **National legislation.** Any restriction on right to information must be present in the applicable national legislation | Ley de Acceso a la Información Pública (LAIP 2008)<br>Article 69 overrides conflicting legislation, but 19(2) and 20(4) allow information to be classified by other laws. |
| **Exceptions related to defence.** The exceptions to the right of access based on national security are well-defined and consistent with international standards. | Article 23 of the LAIP establishes that information may be classified as reserved when its disclosure could jeopardise national security, the defence of the State, or compromise military or police operations.<br><br>A separate category of restricted information, "confidential," may apply to the defence sector in some circumstances.[48] |
| **Harm test.** Information may be exempted from disclosure only if there is a real and substantial likelihood that its disclosure could cause serious harm | A harm test exists in the legislation. When a government agency seeks to categorize information as classified, the LAIP mandates fulfillment of the following three requirements:<br>1. The information falls under at least one of the defined reasons for classification.<br>2. Release of the information threatens an interest protected by the LAIP.<br>3. The damage or harm that may occur from publishing the information outweighs the public interest. |
| **Public Interest Test.** The law should provide for a balancing test (harm of disclosure vs public interest in disclosure) when information is requested | The public interest is considered as part of the harm test (see above). The public does not appear to have access to information once it is deemed classified, although its disclosure may be requested once the established time period has elapsed. |
| **Appeals.** Requesters have the right to lodge an appeal with an independent administrative oversight body. | If a citizen considers that the information should not be classified, he/she may request a review. If the request is rejected, they may appeal the decision to the Human Rights Ombudsman's Office (SECAI) or to the courts. |
| **Declassification.** There should be a maximum expiry time in every secrecy regime | According to Article 28 of the LAIP, when the seven-year classification period is set to expire, the government may extend this period for up to five additional years if it provides a justified legal argument that releasing the information could damage a protected public interest. However, in no case can the information remain classified for more than 12 years.<br><br>In contrast to classified information, confidential (confidencial) information has no expiry period, and can remain indefinitely protected and out of public knowledge. |

48 Information is considered "confidential" in the following ways: (1) As defined by the Law of Banks and Financial Groups (Ley de Bancos y Grupos Financieros) and other laws. (2) When the information is considered a professional secret, sensitive data or sensitive personal data that can only be known by the right holder. (3) When information about individuals is registered by a public institution under guarantees of confidentiality.

Antigua Guatemala, (Photo Credit: Jeison Higuita, Unsplash)

Between 2014 and 2017, more than 90 percent of the requests of access to information made to public institutions were resolved favorably and the information was released. [49] Yet, security and defence institutions still have to fully comply with the obligations established by law, particularly on information related to budget execution, the list of civil servants and public employees, fees, salaries of public officials and employees, remunerations and contracting of goods and services.

The 2023 annual report by SECAI analysed the level of compliance of public sector institutions based on their resolution of information requests. In 2023, the Ministry of Defence received 615 requests, with a compliance level of 88.16 percent. However, no details are given as to why this score was given or what type of information was restricted. In addition, the law (LAIP 2008) contains exceptions to restrict information that jeopardises national security. Therefore, if the MoD restricts information, it is still compliant with the law and the compliance results are not affected.

Inadequate management of public archives has resulted in delays in compliance with the LAIP, in addition to the loss of important archival information. SECAI has called for regulations to improve standardization in information management among government institutions in order to ensure that institutions adequately and effectively manage their archives SECAI and the Human Rights Ombudsman (PDH), its controlling organisation, have urged lawmakers to approve draft bill 4307, the proposed National Archives Law (Ley Nacional de Archivos).This bill includes the creation of the National Archives System to coordinate and manage archives processes; the establishment of the General Archive of the Nation to support public institutions in the management of their archives, and the protection of historical documents key to justice on human rights.

## Defence Finances

Budget transparency in Guatemala is comprehensive (See table below). The Ministry of Finance publishes the approved budgets for the fiscal year on its website, and there is a Budget Transparency Portal that provides citizen documents and the budget in open data format. The defence budget breakdown includes details on military and security equipment, salaries of permanent and contract personnel, remunerations, training services, infrastructure maintenance, and administrative expenses. The budget breakdown is organised by governmental sections, and can be filtered by governmental institution. It includes also an explanation (for experts) on the distribution of the budget for the fiscal year. It does not, however, include expenditures for research or disposal of assets.

While approved budget information cannot be classified by contract, there are databases from 2016 to 2024 with information on public tenders for procurement. The data is disaggregated by purchasing unit within the Ministry of Defense (MoD), the description of the procurement, modality, date of publication, and closing date of reception.

49 WOLA. "Transparency in Guatemala: Assessing Access to Public Information." Central America Monitor. Washington DC, October 2019.

There are no other sources of income for the defence sector other than the central government allocations. The Ministry of Defence does not formally own any companies and there is no defence industry in Guatemala.

The Budget Transparency Portal provides updates on the execution of the budget during the fiscal year, but does not include explanations or clear language for non-experts. While there is no specific analysis or report of variations between the budget and its execution, the Year-End Report (Informe de Fin de Año)—an analysis is conducted by the central government and covering the main public programmes—includes a section that highlights the executed budget relative to the approved budget, referred to as the "percentage of execution".[50]

**Table 6: Open Budget Index scores among ATI case studies, International Budget Partnership 2023**

| Country | Transparency Score (out of 100) | Rank (out of 125 countries) | % change since last index[51] |
|---|---|---|---|
| **Mexico** | 80 | 6 | 3% |
| **Brazil** | 80 | 7 | no change |
| **Dominican Republic** | 77 | 12 | no change |
| **Peru** | 71 | 18 | 16% |
| **Guatemala** | 64 | 29 | no change |

**Table 7: Military expenditures among ATI case studies, SIPRI 2023[52]**

| Country | Military spending (USD millions) | % change 2022-2023 | % change 2014-2023 | Per capita spending | % of government spending |
|---|---|---|---|---|---|
| **Mexico** | 11825.9 | 17% | 75% | 92.1 | 2.37% |
| **Dominican Republic** | 893.2 | 17% | 104% | 78.8 | 3.92% |
| **Honduras** | 539.8 | 18% | 123% | 51.0 | 5.86% |
| **El Salvador** | 453.7 | -1% | 94% | 71.3 | 4.66% |
| **Guatemala** | 422.3 | -4% | 72% | 23.3 | 2.98% |

50 Ministry of Defence. "Informe de Fin de Año (Year-End Report)." Guatemala, 2023.

51 The +/- indicates whether the Transparency Score rose or fell against the last iteration of the Open Budget Index.

52 Average % of government spending: Latin America and the Caribbean: 4.08% (Colombia is highest at 8.31%)

### Snapshot: Guatecompras

The information on the tenders of the Ministry of Defence includes the tender description, the category (item), the type of tender, the type of bids, the date of submission, and the type of process and status. There is also information on the award process that includes the list of bidders, and the company that won the contract (name and amount of the contract).

The information is published without exceptions, but without indication of what is not published. While it is possible to see the name of the supplier, the amounts executed and paid neither the date of payment, nor the date of delivery, nor any contract modifications is published.

Some examples of the procurement purchases by the Ministry of Defence include food and seeds; computers and telecommunications; banking services; clothing and footwear; transportation; airline tickets and rifle cases. The portal is not used for munitions and armaments tenders.

## Defence Procurement

Routine defence procurement in Guatemala is conducted via the online procurement portal, *Guatecompras*–the official portal of the government of Guatemala for the management of public procurement and contracting. Tender and award information is also available for purchases of weapons and tactical equipment, including suppliers and type of tendering procedure used.

According to the provisions of the National Contracting Law, Decree No. 57-92, all public entities must use the portal for purchases, suppliers and contracts, including the Ministry of Defence. The portal is connected to an open contracting Application Programming Interface (API) that adopts the Open Contracting Data Standard (OCDS).[53] The OCDS portal publishes information in open data (XLS, CSV, JSON format).

The Ministry of Defence has oversight of private sector activities through its pension investment fund, Instituto de Previsión Militar (Military Penson Institute or IPM), which owns controlling stakes in several companies, including a firm that supports the production of industrial explosives, Maya Quimicos,  and has received several lucrative contracts from the Ministry of Defence.[54] The IPM has been recently accused of improper handling of nearly USD20m in assets and credits, including[55] unpaid loans, the operations of companies that do not report profit, the existence of properties no longer in use, and concessions managed by private companies that do not declare their income.[56]

While not overseen by the Ministry of Defence, military influence in private security is pervasive in Guatemala. The proliferation of private security companies, many of them founded or operated by ex-military personnel, is a way for former armed forces members to influence the market. In the last 14 years, the Guatemalan state has spent 3.3 billion Quetzals (approximately 437 million USD) in contracts awarded to private security companies.[57] The names of the most benefited contractors are constant and repeated year after year, pointing to a market dominated by retired military personnel.

## Transparency for Civic Engagement in defence matters

The national security policy is based on the Strategic Plan and the Strategic Agenda for National Security. Both the strategic agenda and the national security policy have involved inter-institutional consultations, but there is no evidence of a formal public consultation process occurring on a regular basis. For instance, the National Security Strategic Plan 2020-2024 was coordinated by the Advisory and Planning Commission of the National Security Council (CSN) with insights from the Technical Secretariat of the CSN, the National Security System, the Planning Secretariat of the Presidency, and the Ministry of Public Finance. The revision of the security strategy does not involve a formal public consultation process.

53 The Open Contracting Data Standard (OCDS) is a free, non-proprietary open data standard for public contracting, implemented by over 30 governments around the world. It describes how to publish data and documents about contracting processes for goods, works and services.

54 Garcia, Christian. "Militares Reciben Más de Q6 Millones Con Una Empresa de Explosivos." *Prensa Comunitaria*, August 9, 2024.

55 Balsells, Edgar. "IPM: Golpe Tras Golpe Con Dineros Del Fisco." *Plaza Pública*, February 15, 2024.

56 Cuevas, Douglas. "La CGC sanciona y denuncia al IPM por irregularidades en Q159.7 millones." *Prensa Libre*, February 8, 2024.

57 Chavez, Suchit. "Los Dueños de La Seguridad Privada En Guatemala." *Plaza Pública*, March 10, 2019.

The current formulation of the National Security Policy 2024 has involved the participation of various state institutions, including the Ministry of Government and deputies from the current governing Semilla party. Although many stakeholders participate in the formulation of security and defense policies, these processes tend to be more inter-institutional rather than broad and formalised public consultations.

Guatemala's National Defence Policy 2021-2032 includes sections that address interaction and cooperation with civil society. On issues of transparency and access to information, the policy establishes commitments to ensure that information on defence is available and accessible to the public. This includes the publication of strategic documents and activity reports, allowing civil society to monitor the Ministry of Defence actions. The policy also highlights collaboration with NGOs and international organisations working in areas related to human rights, security and development, but it does not establish clear mechanisms, such as consultations or regular forums.

**Table 8: Access to key documents related to defence matters - Guatemala**

| Information | Public availability | Additional explanation |
|---|---|---|
| **Defence Strategy/Policy** | The MoD publishes defence policy, strategic plans and annual reports that are available for public consultation.<br><br>The Technical Secretariat of the National Security Council publishes strategic documents, including national security policies as well as the Strategic Agenda and Strategic Plan. | Examples of accessible documents: (1) National Defense Policy 2021-2032; (2) National Security Policy 2017; (3) Strategic Security Plan and Agenda; (4) National Security Policy 2024 (working groups to define the new policy). |
| **Audit reports** | The General Audit Office (CGC) of Guatemala publishes annual and ad hoc Audit Reports, which detail the reviews conducted on the use of public resources, including procurement and contracting in the defence sector. | The CGC has inspected and reported on the procurement process of weapons purchases (Argentinian jets in 2019) as well as the current investigation into the dealings of the IPM (See above). |
| **Asset Disposals** | There is no information made publicly available about the results of the disposal of assets, either by the Ministry of Finance or Ministry of Defence. | Although government entities are obliged to maintain transparency in the information related to the asset disposals, the information may be subject to restrictions due to national security considerations |

# Recommendations for civil society, academics, experts, media, and policymakers

1. Advocate for the continued independence and operational integrity of SECAI to safeguard access to information, especially given the previous threats to democratic institutions and transparency.[58]

2. Identify alternative measures for the enforcement of access to information legislation that circumvent the involvement of the Public Prosecutor's Office. Possibilities include:

   a. Implement legal action against non-compliant bodies/institutions. Although the process can be lengthy, it is relevant to ensure the compliance of the LAIP by implementing a *de facto* enforcement.

   b. Consider recognition for public agencies that perform effectively on ATI requirements using the Compliance Level score (NC-IPO), and awards for public officials that positively support ATI implementation.

   c. Requiring minimum level of access to information by government agencies before budget allocations is released, which would require the involvement of the Ministry of Finance.

3. Advocate for the approval of draft bill 4307, the proposed National Archives Law (Ley Nacional de Archivos), so as to reform the information classification system. This legislation would enhance transparency and access to information, playing a crucial role in historical truth and justice, particularly concerning human rights.

4. Engage with the Ministry of Defence and relevant Parliamentary Committees on issues of defence, including requesting inputs to defence strategies and policies, discussions of defence acquisitions, and aspects of defence oversight.

5. Advocate for clearer explanations regarding classified defence information and the compliance of the Ministry of Defence. Although the Compliance Level score provides insights into the resolution of information requests, the annual reports should explain details whether there was denied information by the MoD and what type of information was restricted or denied.

58 See the advocacy guide published by TI-DS in 2024 for an in-depth review of tactics and approaches to establishing access to information in the defence sector: Transparency International Defence & Security. "Defending Transparency: An Advocate's Guide to Counteracting Defence Corruption." London, 2024. https://ti-defence.org/publications/defence-security-sector-advocacy-toolkit-guide/.

CASE STUDY

# MALAYSIA: ACCESS TO INFORMATION IN THE DEFENCE SECTOR

## Overview

1. Malaysia experienced its first peaceful transition of power in 2018, but since then, has stalled on a number of governance reforms, including access to information. The Official Secrets Act 1972 (OSA) functions as the de facto national framework for access to information and overrules any other legislation on information access.

2. Malaysia has struggled with corruption, losing billions of dollars in the state development fund 1MDB in 2015, and more recently in the Littoral Combat Ship scandal of 2022. A lack of parliamentary oversight of state-affiliated companies and investment funds, as well as the close relationship between the public and private sectors, has historically created conditions conducive to corruption.[59]

3. There is little information about the defence budget or expenditures, and almost no publicly available information about acquisition planning. Auditor General reports are the primary means by which financial information is released about defence activity, and otherwise, information is pieced together from publicly available audit reports, media reports about defence weapons and equipment purchases, whistleblowers, and corruption scandals in the news.

4. The Malaysia Defence White Paper of 2020 (DWP), prepared through discussions and public engagements, calls for increasing public awareness of defence-related matters. However, little engagement with civil society and the public has happened since its publication.

## Country Context

Malaysia has yet to pass an access to information law, though two of its states have done so in 2010 and 2011, albeit with lackluster implementation.[60] The Official Secrets Act 1972 (OSA) functions as the de facto national framework for access to information and overrules any other legislation on information access.

In general, information on acquisitions for any military and defence-related projects is not made public. The details of acquisitions or the associated process rarely appear to even be disclosed at the parliamentary level. MPs not only have limited information to engage actively in parliamentary debates, but there were instances where questions from MPs on the budget or the maintenance cost of defence assets were rejected by the House Secretary on the grounds of the OSA.[61] This practice has led to limited available information, for example through public write-ups or academic journal articles destined for public consumption.

59 "Over $1 Billion in Misappropriated 1MDB Funds Now Repatriated to Malaysia." Washington DC: United States Department of Justice, August 5, 2021; Alecci, Scilla. "Malaysian Politician under Pandora Papers Probe Linked to $52 Million Offshore Trust and UK, US Property Investments - ICIJ." *International Consortium of Investigative Journalists*, January 17, 2024; Global Witness. "The Real Wolves of Wall Street," 2017.

60 Ling, Gan Pei. "Why so Secretive, Civil Society Asks Selangor, Penang." *The Malaysian Insight*, October 31, 2017.

61 Chin, Jitkai, Liew, Chin-Tong, and Mohammad, Nur Jazlan. "Role of Parliament in Defence Budgeting in Malaysia." *Geneva Centre for Security Sector Governance (DCAF)*, 2007. https://www.dcaf.ch/sites/default/files/imce/APU/RoleParliamentMalaysia.pdf

## MALAYSIA HAS STRUGGLED WITH CORRUPTION

### LOSING BILLIONS OF DOLLARS IN THE STATE DEVELOPMENT FUND 1MDB IN 2015, AND MORE RECENTLY IN THE LITTORAL COMBAT SHIP SCANDAL OF 2022

Malaysia has proposed a 10% increase in its 2024 defence budget, in part to fund the procurement of new combat aircraft and drones, but also to modernise aging equipment and infrastructure.[62] With a history of corruption in defence procurement, concerns have been raised by Transparency International Malaysia that, without stringent rules on the role of intermediaries in decision-making, increased spending will lead to fraud and embezzlement.[63]

Since the Littoral Combat Ship (LCS) scandal was revealed in 2022, the Ministry of Defence (MINDEF) has increased the frequency of public updates on the construction status of the revitalised LCS project,[64] demonstrating a commitment to preparing and submitting periodic progress reports to the Cabinet, in line with the conditions set by the Auditor General.[65] However, this shift is likely a one-off response driven by the high-profile nature of the scandal, which provoked widespread public awareness and outrage. Transparency and regular updates on defense-related procurements have not yet been a standard practice for MINDEF.

#### Littoral Combat Ships Scandal (2011 – present)

Beginning in 2011, the Malaysian government has endured an evolving scandal involving the purchase of six littoral combat ships from Boustead Naval Shipyard, a former subsidiary of MINDEF-owned holding company Boustead Holdings, now fully owned by the Ministry of Finance:[66]

- In 2011, the government under Prime Minister Najib Razak's administration, approved the Navy's request for six littoral combat ships (LCS) in a deal worth at least RM9.13 billion (USD2.1b). It was the most expensive defence contract in history. Ahmad Zahid Hamidi was then minister of defence.[67]
- In 2013, the contract was awarded to Boustead Naval Shipyard Sdn Bhd (BNS) without an open tender being called.
- More than 10 years later none of the ships have docked on the shores of Lumut. The Public Accounts Committee found that the completed detailed design of the ships was still yet to be seen in August 2022, even though 66.64% (or RM6.1 billion) of the RM9 billion had been paid to BNS.
- Investigations by the Public Accounts Committee into the project show red flags: from Boustead Naval Shipyard, a company in a critical financial state; unheeded advice from the Royal Malaysian Navy, who did not get to choose the design of the ship that they would be using; and a middleman, who allegedly marked up the project cost by up to 4 times its initial value.
- On 11 August 2022, the Malaysia Anti-Corruption Commission handed over its investigations on the project to the Attorney-General, with recommendations of charges to be filed against individuals linked to the project.

62 Huxley, Tim. "Malaysia's defence policy under the Anwar government." *International Institute for Strategic Studies*, September 8, 2023.

63 New Straits Time. "TI-M questions sudden silence over the Littoral Combat Ships (LCS) project." May 29, 2023.

64 Bernama. "Second Lcs 64.66 Pct Complete, Says Defence Minister." June 24, 2024.

65 Free Malaysia Today. "Finance ministry establishes SPV to take over BNS." May 26, 2023.

66 Yunus, Arfa. "LCS Scandal: Report Reveals Zahid Involved in Procurement Process." *NST Online*, August 17, 2022; Sipalan, Joseph. "Will Missing Ships Scandal Sink Malaysian PM's Team, Umno Leadership?" *South China Morning Post*, August 16, 2022, sec. This Week in Asia.

67 BFM Media. "The Littoral Combat Ship Project: How It Went Wrong, Explained." *BFM The Business Station*, August 11, 2022.

### Littoral Combat Ships Scandal (2011 – present) *continued*

- Former Royal Malaysian Navy (RMN) chief, Tan Sri Ahmad Ramli Mohd Nor, who was the managing director of Boustead Naval Shipyard (BNS) at the time, is currently being charged in court with three counts of criminal breach of trust for authorising payments of more than RM21 million to three Singaporean companies without the approval of BNS's board of directors.[68] However, several other key figures allegedly involved in the misappropriation of funds and abuse of power in the ship procurement process have not been investigated by the authorities.
- Malaysia is on track to receive its first Littoral Combat Ship by 2026, with overall costs for the project rising to RM11.22b (USD2.56b), even though the order was reduced to five ships.[69]

Efforts to pass transparency-related reforms have been ongoing for years.[70] In September 2023, the Special Cabinet Committee on National Governance (JKKTN), chaired by Prime Minister Datuk Seri Anwar Ibrahim, agreed in principle to the enactment of a freedom of information bill.[71] This also includes potential amendments to the Official Secrets Act (OSA) to align it with the forthcoming bill. The drafting and consultation process for the freedom of information bill is currently underway, with the aim of tabling it in Parliament by the end of 2024.[72]

## RTI law and classification

In the absence of a national access to information law, the Official Secrets Act 1972 (OSA) serves as the controlling legislation, which prohibits the dissemination of information classified as secret. The states of Selangor and Penang have adopted Freedom of Information Acts, but both laws are superseded by the OSA if a piece of information has been designated as an official secret. In fact, enactment of a freedom of information law would necessitate the amendment of several provisions of the OSA in order for the information to be disclosed freely. Despite the Malaysian government's ongoing plans to enact a Freedom of Information Bill, there are still no clear plans on how the Official Secrets Act (OSA) will be amended.

Kulala Lumpur, Malaysia (Photo Credit: Pexels, Pixabay)

68 Center to Combat Corruption and Cronyism (C4 Center). "The Littoral Combat Ship (LCS) scandal – the crooks and villains behind Malaysia's defence procurement laid bare." September 21, 2022.

69 Loheswar, R. "Malaysia's First Littoral Combat Ship to Be Delivered by 2026, Defence Minister Reassures after Delays." *Malay Mail*, August 21, 2024.

70 "Malaysia: Freedom in the World 2024 Country Report." Freedom House, 2024.

71 Prime Minister's Office of Malaysia. "Enactment of Freedom f Information Act Approved in Principle – PM Anwar." September 14, 2023.

72 Malay Mail. "Freedom of Information Bill to Be Tabled in Parliament by End of This Year, Says Deputy Minister." July 16, 2024.

**Table 9: Key features of ATI legal frameworks - Malaysia**

| | |
|---|---|
| **National legislation.** Any restriction on right to information must be present in the applicable national legislation | Official Secrets Act (1972)<br>No national ATI law, but states of Selangor[73] and Penang[74] have adopted ATI laws. |
| **Exceptions related to defence.** The exceptions to the right of access based on national security are well-defined and consistent with international standards. | The Schedule to the Official Secrets Act lists three categories of documents that are always considered 'official secrets': (1) Cabinet records, records of decisions and deliberations including those of Cabinet committees; (2) State Executive Council documents, records of decisions and deliberations including those of State Executive Council committees; (3) Documents concerning national security, defence and international relations.<br>Under section 2A, this list may be added to at any time by Ministerial Order. |
| **Harm test.** Information may be exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm | None. Based on absolute exceptions rather than a specific harm. |
| **Public Interest Test.** The law should provide for a public interest test when classified information is requested | None in the Official Secrets Act.<br>Both Penang[75] and Selangor's[76] ATI laws include an exemption clause that allows for the disclosure of restricted information if the public interest outweighs the potential harm. However, since these laws apply only to information and decisions within the states' jurisdiction and cannot override other existing laws, such as the Official Secrets Act (OSA), the scope and effectiveness of the public interest test remain highly debatable. |
| **Appeals.** Requesters have the right to lodge an appeal with an independent administrative oversight body. | None. |
| **Declassification.** There should be a maximum expiry time in every secrecy regime | There is no expiry time for classified information. Art 2c of the Official Secrets Act states that any public officer may, at any time, declassify any document specified in the Schedule or any official document, information or material that has been classified as an official secret. |

Since 2015, Malaysia has a government-run open data platform that serves to improve governmental transparency (data.gov.my). However, government data management remains highly decentralised. With every agency having the authority to decide what data can be shared,[77] the Ministry of Defence (MINDEF) can withhold much of the information that would be of public interest.

Although MINDEF publicly strives to be more transparent, they have not uploaded any information related to the Ministry on the national open data platform. Information requests related to defence and security are routinely denied for reasons relating to national security, as required by the OSA.

73 Freedom of Information Act (Selangor State) 2011.

74 Penang Island Information Enactment 2010.

75 Penang Island Information Enactment 2010, art 15(1)(a).

76 Freedom of Information Act (Selangor State) 2011, art 14(2)(a).

77 Shahrudin, Ashraf. "Open Government Data in Malaysia: Principles, Benefits, Challenges and the Way Forward." In *#Networked Nation: Navigating Challenges, Realising Opportunities of Digital Transformation*, 103–35. Kuala Lumpur: Khazanah Research Institute, 2021.

Tank on Military Parade, Kuantan, Malaysia (Photo Credit: Din Aziz, Pexels)

## Defence Finances

The defence budget is available online via the Ministry of Finance's website. However, it is a general budget outlining related functions without a comprehensive expenditure breakdown across them. In fact, much of the defence budget information is in aggregated form and without defence-specific explanations, as is common for documents relating to national security, which are protected under the Official Secrets Act.

Moreover, the formulation of the annual defence budget is done internally by the Ministry of Defence (MINDEF) and is submitted directly to the Budget Division of the Treasury.

The totality of the defence budget comes from the central government and there are no other sources of defence income. All proceeds from equipment sales or asset disposals are collected into consolidated funds, which do not belong to MINDEF but are not released publicly either.

The Ministry of Defence's annual spending is outlined in the National Budget Estimate by the Ministry of Finance. All ministries are required to submit a budget request which shows how much is needed per line item. However, in the case of MINDEF, there is no indication that this should be made public or even disclosed to Parliament.

Spending is not published for public consumption but is subject to the Auditor General's Office annual auditing processes.

MINDEF does have oversight of private sector activity through its pension investment fund, Armed Forces Fund Board (LTAT), which owns controlling stakes in several publicly-listed Malaysian firms, including Boustead Holdings and Afin Holdings. As of 2023, LTAT had USD2.6 billion in assets under management.[78] These businesses are publicly declared, and some are military-majority owned companies that are traded on Bursa Malaysia. They are subject to rules and regulations of the Securities Commission Malaysia. Like other publicly listed companies, all of LTAT's subsidiary companies are required to report their operational balance sheets and yearly financial results, which have to be submitted to the Securities Commission of Malaysia. The yearly financial statements are also posted online on the website for public consumption.

Several of these LTAT subsidiaries have come under scrutiny for mismanagement and misuse of funds for election campaigns.[79] Boustead Holdings, for example, has seen a government takeover of much of its governance, as well as some of its subsidiaries, as its firms continue to collapse under mismanagement.[80]

78 Barrock, Jose. "The LTAT Conundrum." *The Edge Malaysia*, May 13, 2024.

79 M. Shanmugam. "Fort LTAT Breached." *The Star Online*, April 13, 2019.

80 Guild, James. "Why the Malaysian State Is Taking Firmer Control Over Boustead Holdings." *The Diplomat*, October 17, 2023; Guild, James. "Why Malaysia's Pharmaniaga Is In Financial Trouble." *The Diplomat*, February 20, 2024.

Table 10: Open Budget Index scores among ATI case studies, International Budget Partnership 2023

| Country | Transparency Score (out of 100) | Rank (out of 125 countries) | % change since last index[81] |
|---|---|---|---|
| **Philippines** | 75 | 15 | 10% |
| **Indonesia** | 70 | 20 | no change |
| **Mongolia** | 62 | 36 | 3% |
| **Thailand** | 60 | 43 | 3% |
| **Malaysia** | 48 | 65 | 2% |

Table 11: Military expenditures among ATI case studies, SIPRI 2023[82]

| Country | Military spending (USD millions) | % change 2022-2023 | % change 2014-2023 | Per capita spending | % of government spending |
|---|---|---|---|---|---|
| **Singapore** | 13200.7 | 10% | 38% | 2194.6 | 18.03% |
| **Indonesia** | 9480.8 | -6% | 37% | 34.2 | 3.92% |
| **Thailand** | 5765.8 | -4% | 3% | 80.3 | 4.92% |
| **Philippines** | 5451.7 | 2% | 76% | 46.5 | 5.02% |
| **Malaysia** | 3899.1 | 6% | -21% | 113.6 | 4.11% |

## Defence Procurement

There is no public procurement law as such, though a draft is being produced.[83] As a result, public oversight over the procurement process is limited, with the Public Accounts Committee (a parliamentary oversight body) only allowed to ask questions and make recommendations. There is evidence of some oversight of procurement (e.g. reports, announcements in the press of the cancellation of procurement programmes, the release of financial information), but information is only available to the parliamentary committee or the Auditor General's Office.

Guidelines and procedures for general tenders and procurements are available online, though only specific information is available to the public, i.e. procurement advertisement/tender and disposal of non-strategic assets. Tender processes relating to strategic military procurement are not available to the public.

Malaysia has struggled with corruption in procurement across government,[84] with the most recent case of bid-rigging in defence procurement announced in December 2023. An investigation by the Malaysia Competition Commission (MyCC) found seven enterprises had colluded in their bid submissions for four tenders issued

81 The +/- indicates whether the Transparency Score rose or fell against the last iteration of the Open Budget Index.

82 Average % of government spending: Southeast Asia: 8.64% (Singapore is highest at 18.03%)

83 *The Star*. "Government Procurement Bill to Be Drafted, Says PMO." Sep 2023.

84 Malaysian National News Agency. "MACC: Rampant Corruption in Govt Procurement Processes." *NST Online*, September 30, 2020.

by the Ministry of Defence for provision of goods and services worth about RM20.8 million (USD4.8m). Its investigations also revealed that the firms had engaged in bid rigging through the exchange of information, facilitation of tender submission and subcontracting as a kickback.[85]

Some procurement tenders are advertised on the Defence Ministry's website, but their results are not made public. Changes or modifications to a project are subject to a review by the Technical and Financial Committee, and must be reported to the procurement committee if the value of the overall project exceeds "RM50 million for supplies and services and RM100 million for works for Government Ministries/ Departments." However, the modifications are not available publicly.

Some weapons and armaments purchases are made public through ad hoc means, typically at the two larger defence exhibitions in Malaysia, Defense Services Asia (DSA) and the Langkawi International Maritime and Aerospace Exhibition (LIMA), while other major defence purchases have been disclosed in Parliament. The media may also occasionally report on purchases made, but details on the purchases are not extensive. The lack of transparency is typically justified by national security concerns and details are kept secret under the Official Secrets Act.

**AN INVESTIGATION BY THE MALAYSIA COMPETITION COMMISSION (MYCC) FOUND**

**SEVEN ENTERPRISES HAD COLLUDED IN THEIR BID SUBMISSIONS**

**FOR FOUR TENDERS** ISSUED BY THE MINISTRY OF DEFENCE FOR PROVISION OF GOODS AND SERVICES WORTH ABOUT

**RM20.8 MILLION (USD4.8M)**

## Transparency for Civic Engagement in defence matters

The Malaysia Defence White Paper of 2020 (DWP) was prepared through discussions and engagements with the public, non-governmental organisations (NGO), defence industry players, academics, and other ministries involved in the defence landscape. A technical team consisting of members of the ministry's policy planning division and related departments, representatives of all three services of the armed forces, researchers of the Malaysian Institute of Defence and Security (MiDAS), as well as academics in the field of strategic studies from local universities discussed the directions and details of the DWP with stakeholders. Some 21,000 respondents participated in an online survey conducted by MiDAS. The Ministry also made an effort to ensure extensive engagement beyond the government. For instance, it set up a special booth during the Langkawi International Maritime and Aerospace Exhibition (Lima 2019) to allow visitors to contribute ideas to the DWP. An Experts Panel was also involved in discussions with MINDEF. The inputs from all these channels were debated in-depth at various fora, with some issues brought to ministerial level meetings for incorporation into the DWP.

Beyond the formulation of the DWP, the military does not usually engage with CSOs in anti-corruption matters. Investigations of anti-corruption may be called for by CSOs and submitted to the Malaysian Anti-Corruption Commission (MACC) and other bodies, but the process is led predominantly by the MACC or other governmental institutions not related to defence.

The DWP emphasised the importance of good governance, under its tagline "*Achieving Best Governance Standards*,"[86] and the implementation of checks and balances based on the principles of transparency and accountability as key to its success. It also identified increasing public awareness of defence-related matters as crucial for gaining support for Malaysia's ambitious national defence transformation plans. Yet, the DWP do not provide clear guidelines on how public awareness and accountability are to be achieved, a shortcoming likely due to the constraints imposed by the OSA.

85 *The Star*. "Mindef Submits Documents Linked to Probe on Alleged Bid-Rigging by Seven Companies." December 21, 2023, sec. Nation.

86 "Defence White Paper (Kertas Putih Pertahanan)", Ministry of Defence Malysia, 2020.

Table 12: Access to key documents related to defence matters - Malaysia

| Information | Public availability | Additional explanation |
|---|---|---|
| **Defence Strategy/Policy** | The Malaysia Defence White Paper of 2020 and National Defence Policy of 2010 are both available online. | Once a draft document has been completed, there is no provision for enabling the wider community to review that draft and contribute comments to strengthen it.<br><br>The practice is often to place the entire process under the Official Secrets Act (OSA).[87] |
| **Audit reports** | The Auditor General's reports on the defence sector are available online. | MINDEF has repeatedly failed to address the issues highlighted in the Auditor General's reports. |
| **Asset Disposals** | Public Asset disposals at the Ministry are related only to non-sensitive defence items like trucks, cars, outdated computers etc. There is no information on how strategic assets such as weapons are disposed of. | It is not a practice of any ministries in Malaysia to disclose the amount of money received from disposal exercises. |

## Recommendations for civil society, academics, experts, media, and policymakers

1. Continue to advocate for the development and enactment of an access to information law,[88] building on Prime Minister Ibrahim's public commitment to do so.[89]
   a. Ensure that the ATI law includes clear balancing tests to establish harm or public interest in the disclosure of information.
   b. Advocate for the establishment of an independent appeal body to assist with implementation throughout the public sector and to clarify rules on access to information.
2. Advocate for reforming the Official Secrets Act so that exceptions for national security matters adhere to the Tshwane Principles.
3. Advocate for public discussions of defence matters with the involvement of MINDEF officials, emphasising that this will increase public awareness of national defence transformation plans.
4. Commission a "lessons learned" review of the experiences in implementing state-level access to information laws in Penang and Selangor, to identify challenges or priorities in current initiatives at the national-level.
5. Advocate for the Ministry of Defence (MINDEF) to publish expenditure data on the national open data platform (data.gov.my) and encourage public awareness of MINDEF's spending, and greater accountability and transparency in defense budgets and financial management.

87 "Open Letter To PM: Reform Lawmaking Process - 40 Activists & CSOs." CodeBlue, January 3, 2024.

88 See the advocacy guide published by TI-DS in 2024 for an in-depth review of tactics and approaches to establishing access to information in the defence sector: Transparency International Defence & Security. "Defending Transparency: An Advocate's Guide to Counteracting Defence Corruption." London, 2024. https://ti-defence.org/publications/defence-security-sector-advocacy-toolkit-guide/.

89 Prime Minister's Office. "Enactment of Freedom of Information Act Approved In Principle." Kuala Lumpur, September 14, 2023.

CASE STUDY

# NIGER: ACCESS TO INFORMATION IN THE DEFENCE SECTOR

## Overview

1. The 2023 coup d'etat in Niger has led to increased violence, stark reductions in foreign assistance, and a severe curtailing of access to information and other democratic rights.
2. Although there is no national law regulating access to information, there is an Order (No. 2011-22), with limited scope and no implementation mechanisms. The national ombudsman has undertaken efforts to implement the order, but lack of resources constrain its impact.
3. There are no balancing tests to determine harm of disclosure or benefit to the public interest, resulting in the widespread withholding of information deemed to threaten the "secrecy of national defence, conduct of foreign policy, security of the state, or public safety."
4. Prior to the coup, defence income and military spending were mainly non-transparent, as were defence purchases. A new law (Order No. 2024-05) was passed in 2024 that excludes all defence matters from public procurement, public accounting, and taxes.

## Country Context

In July 2023, the Nigerien military and presidential guards staged a coup d'état, removing and detaining President Mohamed Bazoum, who still remains on house arrest. The resulting political volatility also triggered an escalation in militant Islamist group attacks. The number of deaths from political violence more than doubled compared to the year prior, rising by 121%, while the number of civilian deaths from direct targeting rose by 34%.[90] Niger is now marked by rising insecurity, where "human rights are in free fall."[91]

Niger is among a cohort of countries in Western Africa that have fallen to military coups in the last several years. Western donors have ceased sizable funding operations for these governments, which in turn are rejecting support from governments demanding a return to democratic rule. Russia has stepped in with an increasing amounts of aid to Niger, Mali and Burkina Faso.

In Niger, the junta has expelled French, US, and German forces from the country, leaving it vulnerable to increased attacks from Islamist militants, and encouraging the presence of private military and security companies—such as Russian-backed Wagner (now rebranded 'Africa Corps')—that are tasked with providing security for ruling military juntas and their interests. The junta has reportedly agreed to pay for the deployment of Russian Africa Corps troops by granting gold mining rights. Allegedly, lithium and uranium mines are next, a decision that could strip the country of its rights to its own natural resources and could jeopardize European energy markets.[92]

90 Nsaibia, Ladd Serwat, Ariane Dinalli Francisco, Héni. "Africa Overview: July 2024." *ACLED*, August 12, 2024.

91 *RFI*. "Niger: Un an Après Le Coup d'État, Dégradation de La Sécurité Intérieure et Des Droits Humains." July 26, 2024, sec. afrique.

92 Inwood, Joe, and Jake Tacchi. "Wagner in Africa: How the Russian Mercenary Group Has Rebranded." *BBC*, February 20, 2024, BBC Newsnight & BBC Eye Investigations.

People riding on camels in Ingall, Agadez, Niger (Photo Credit: Pexels, André)

Niger has also seen a dramatic tightening of the media and information space under the junta. In January 2024, Association Maison de la Presse (an umbrella association of 32 professional media organisations) was shut down after "denouncing the interruption of democracy and calling on the military to respect fundamental freedoms."[93] In the years leading up to the coup, Niger's digital media platforms were inundated by Russian-linked networks using coordinated techniques to distort information about Niger. These interferences escalated as the coup unfolded and continue apace as Russia delivers money and troops to support the junta.[94]

No roadmap for democratic transition has been established in Niger as of now. The inclusive national dialogue announced in August 2023 has not yet taken place. The activities of political parties remain suspended, with no prospect of resumption.[95] Elected bodies have been dissolved, including at the local level.

A recent presidential decree has also repealed the former procurement law and removed all controls on defence-related spending, inviting significant risk of corruption in defence purchases across all categories of procurement.[96]

## RTI law and Classification

A government decree (Ordonnance 2011-22) stipulates access to information in Niger. It separates administrative documents into "communicable" and "noncommunicable" categories, reflecting different levels of state secrecy. However, it does not provide any explicit provisions for classification. Niger also lacks implementing legislation to support the institutionalisation of transparency within the public sector, leaving investigative media as the sole means of obtaining information.

93 *Africa Center for Strategic Studies*. "Niger Coup Reversing Hard-Earned Gains." May 13, 2024.
94 *Africa Center for Strategic Studies*. "Mapping a Surge of Disinformation in Africa." March 13, 2024.
95 *Le Monde*. "Mali's Junta 'suspends' Political Party Activities for 'Reasons of Public Order.'" April 11, 2024.
96 *APAnews - African Press Agency*. "Niger Keeps Defence Budget under Wraps." March 12, 2024, sec. News.

**Table 13: Key features of ATI legal frameworks - Niger**

| | |
|---|---|
| **National legislation.** Any restriction on right to information must be present in the applicable national legislation | No national RTI law, but there is an Order[97]: Portant Charte d'accès l'information publique et aux documents administratifs (Ordonnance No 2011-22) |
| **Exceptions related to defence.** The exceptions to the right of access based on national security are well-defined and consistent with international standards. | Art 13 states that administrative information or documents may not be consulted or communicated if their disclosure would infringe upon: the secrecy of the deliberations of the Government and the responsible authorities falling under the executive branch; the secrecy of national defense; the conduct of Niger's foreign policy; the security of the State, public safety or the safety of individuals. |
| **Harm test.** Information may be exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm | None. Based on absolute exceptions rather than a specific harm |
| **Public Interest Test.** The law should provide for a public interest test | None |
| **Appeals.** Requesters have the right to lodge an appeal with an independent administrative oversight body. | There is no independent external review body for information access, although citizens can appeal to the "médiateur de la République" (Ombudsman), as per Articles 27–31. However, the external review body has not been operational since the coup d'état in July 2023. |
| **Declassification.** There should be a maximum expiry time in every secrecy regime | None |

Prior to the coup, there was ample activity by civil society organisations to improve the state of access to information in Niger. Much of the work focused on clarifying the definition of state secrets, and allowing oversight institutions to have access to defence-related information. This included the Inspector General, the now-defunct Defence Committee of Parliament, and the Court of Auditors, both of which are no longer operational.

The ruling junta has stated that Niger is subject to existing UN conventions, including the Universal Declaration of Human Rights, which enshrines the freedom of information in Article 19. However, in the current political climate, advocacy for reform around information access is not feasible.

## Defence Finances

The Nigerien defence budget, showing key items of expenditure, is published annually as part of the financial law available in the Official Journal, in a printed and online version. Following the 2023 coup, the government modified the existing finance law but has not yet published the 2024 finance law has in full.

According to the 2018 financial law provisions, which may no longer be applicable, the budget for the Ministry of Defence is divided into three sub-categories: control and administration of national defence policy, securing national territory, and peace consolidation. Relevant categories include recruitment,

97 In Niger, an Ordonnance (Order) is not a ministerial order, nor local or municipal rule, but an act issued by the military authorities with legislative effect nationally. As parliament is suspended, the military concentrates executive and legislative powers.

salaries, training, health services, military infrastructure, maintenance of equipment, armament and munitions acquisitions. In theory, the defence budget should contain comprehensive information on expenses across functions, but some information, notably expenditures by intelligence services, is not detailed and is often marked as "other services and acquisitions".

Prior to the coup, some services related to security and defence responded directly to the Presidency and therefore were not included in the defence budget. They fell under the sub-category "security of the President of the Republic", and included: Presidential Guard, the CNESS, Chief of the Military Staff of the President of the Republic, Directorate General of Documentation and External Security of the State.

Neither the Constitution nor the Military Penal Code bans defence institutions from having beneficial ownership of commercial businesses, but there is no defence industry in Niger. Prior to the 2023 coup, the defence sector was likely financed solely by central government allocations. Post-coup, information on income remains non-transparent, while public contracts for the construction of classrooms, roads, and public buildings are being increasingly awarded to the armed forces.

Military spending is also non-transparent. Reports on the execution of the general state budget exist, but the figures that they outline are highly aggregated and make no reference to specific sectors, ministries, or programmes.

**Table 14: Open Budget Index scores among ATI case studies, International Budget Partnership 2023**

| Country | Transparency Score (out of 100) | Rank (out of 125 countries | % change since last index[98] |
|---|---|---|---|
| **South Africa** | 83 | 4 | -3% |
| **Benin** | 79 | 9 | 22% |
| **Zimbabwe** | 63 | 30 | 7% |
| **Uganda** | 59 | 44 | 2% |
| **Niger** | 33 | 89 | 22% |

**Table 15: Military expenditures among ATI case studies, SIPRI 2023[99]**

| Country | Military spending USD | % change 2022-2023 | % change 2014-2023 | Per capita spending | % of government spending |
|---|---|---|---|---|---|
| **Nigeria** | 3191.9 | 3% | 35% | 14.3 | 5.52% |
| **South Africa** | 2781.1 | -11% | -29% | 46.0 | 2.21% |
| **Angola** | 1270.2 | -22% | -81% | 34.6 | 5.53% |
| **South Sudan** | 1076.2 | 107% | -17% | 97.0 | 8.64% |
| **Niger** | 331.6 | 37% | 128% | 12.2 | 10.23% |

98 The +/- indicates whether the Transparency Score rose or fell against the last iteration of the Open Budget Index.

99 Average % of government spending: West Africa: 7.06% (Burkina Faso is highest at 15.11%)

## Defence Procurement

Gaps in transparency and oversight, combined with a loophole in the procurement law that allows for direct purchases of defence equipment from individuals rather than states, led to severe fraud and embezzlement in Nigerien defence procurement in the past decade. In 2020, a confidential government audit of defence spending found that at least $137m had been lost due to malpractice over an eight-year period ending in 2019. Much of that was lost was due to a series of corrupt international arms deals, in which equipment sourced from international firms (including in Russia, Ukraine, and China) was overpriced, had not been delivered, or had been purchased without a genuine competitive bidding process.[100] The law has since been amended to require only state-to-state procurement for the armed forces.

Since July 2023, no procurement has been published, and from January 2024 an Order (no. 2024-05 of 23 February 2024) with retroactive effect was issued. It excludes the following categories from public accounting, taxes, and public procurement: orders, services and construction work for the defence and security forces, the presidential palace, official residences, and victims of forced displacement.[101] The law also states that acquisitions must come from a restricted list of providers. It represents a drastic blow to oversight of the defence sector, and a further erosion of democratic commitment to transparency and accountability in a sector with rising expenditures and the significant involvement of foreign agents.

Even prior to the coup, Niger faced severe gaps in access to information for defence procurement.

All purchases for the Ministry of Defence (MoD) fell under either the 2016 Code for Public Procurement or under the 2013 Decree that regulated security and defence acquisitions. Acquisitions made under the 2016 Code could be disclosed to the public, but this was not the case for purchases made under the 2013 Decree, which required confidentiality. Purchases of military equipment were often lumped together with in-kind donations or heavily subsidised sales by international partners such as France, Germany, the United States or the European Union. As a result, such purchases were often disclosed by external channels rather than by the government.

Some important acquisitions like helicopters or planes were made public through local or international media. For example, on October 27, 2017, France's Ministry of Defence published a report on its website describing a donation ceremony for a series of armed military vehicles in the presence of Niger's Minister of Defence.[102] Another example was the barracks of the School of Officers of the Nigerien Armed Forces (l'Ecole des Officiers des Forces Armées Nigériennes), which was constructed and equipped by the United States.

Given the confidential dimension of the procurement process, formal oversight mechanisms are not transparent or inexistent. According to Art. 71 of the 2013 Decree, the report of the Inspector General of the Army (IGA) is strictly confidential, and it is forwarded only to the president and the prime minister.

**Gaps in transparency and oversight, combined with a loophole in the procurement law that allows for direct purchases of defence equipment from individuals rather than states, led to severe fraud and embezzlement in Nigerien defence procurement in the past decade.**

100 Burke, Jason, and Jason Burke Africa correspondent. "Niger Lost Tens of Millions to Arms Deals Malpractice, Leaked Report Alleges." *The Guardian*, August 6, 2020, sec. World news.

101 Amnesty International. "Niger: Rights in Free Fall a Year after Coup," July 25, 2024.

102 "Barkhane: la France remet du matériel aux forces armées nigériennes," (Barkhane: France gives equipment to the Nigerien armed forces), French Ministry of Defence, November 6, 2017.

# NIGER HAS A GENERAL POLICY TO FIGHT CORRUPTION, BUT NO SPECIFIC OR CLEAR POLICIES TO COUNTER CORRUPTION IN THE DEFENCE AND SECURITY SECTOR

## Transparency for Civic Engagement in defence matters

When in office, former President Mohamed Bazoum voiced his commitment to countering corruption in public institutions and demonstrated his openness to cooperation with civil society organisations. He reinforced the political independence of the country's official anti-corruption body, the High Authority Against Corruption and Similar Crimes (HALCIA), which was established by decree in 2011. In December 2016, the government adopted a new anti-corruption law that granted the HALCIA more powers, including a right to self-referral, the lifting of bank secrecy, the direct transmission of reports to the public prosecutor, and the launch of public inquiries.

In conclusion, Niger has a general policy to fight corruption, but no specific or clear policies to counter corruption in the defence and security sector. Work done by the previous government in collaboration with the Nigerian civil society and the Geneva Centre for Security Sector Governance (DCAF) achieved several notable transparency reforms: all legal texts and regulations regarding the defence and security sector, as well as a mapping document of all complaints to the Ombudsman regarding the defence and security services was made publicly available (including online).[103]

Formal public consultations on defence policy and the security strategy took place before the 2023 coup, but it remains unclear to what extent defence policy and security institutions incorporated their findings. In the current political climate, there is no public debate over defence policy, nor any consultations with the public or civil society organisations.

**Table 15: Military expenditures among ATI case studies,**

| Information | Public availability | Additional explanation |
|---|---|---|
| **Defence Strategy/ Policy** | A National Security and Defence Policy was developed in 2018, but it is not available publicly.<br><br>The 2011 strategy for development and security (SDS Sahel-Niger) is available online. | According to art. 20 of the 2013 Decree on defence and security procurement, the acquisition plan is not subject to publication and is classified as "top secret". |
| **Audit reports** | Neither the National Audit Office nor the State Inspector General regularly audit defence expenditure or activities. | The Inspector General of the Armed Forces did not share its confidential reports with other oversight bodies, significantly restricting the information available for them to carry out their duties. |
| **Asset Disposals** | There is little to no information publicly available about the process of asset disposal. | There is no indication as to how financial proceeds are incorporated into the budget. Moreover, the National Commission for the Collection and Control of Illicit Weapons is no longer operational. |

103 DCAF. "Enhancing Security Sector Accountability in Niger." Geneva Centre for Security Sector Governance, 2020.

Prior to the 2023 coup, there was considerable advocacy around civic engagement with the defense sector, with several ongoing initiatives:

The **High Authority for the Consolidation of Peace (HACP)** is a government institution created in 1995 that reports directly to the President of the Republic. It is charged with dialogue, mediation, and the implementation of peace accords. Through 2015 – 2018 the HACP initiated and led projects—in the Diffa region affected by the Boko Haram insurgency and on the Malian border—aimed to reinforce dialogue and confidence between the security forces and the local population.

The **National Centre for Strategic Security Studies (CNESS),** created in 2015, is an advisory unit for security and defence policies reporting directly to the presidency. Its governing body, the Orientation Council, decides on proposals regarding security policy. Though CNESS is dependent on the military, it is assisted by a Scientific Council, which includes non-military researchers who provide recommendations on scientific programmes. In December 2017, the CNESS organised the national forum for security and defence to reflect on the security and defence policy developed in 2018. The first forum of its kind, it included representatives from the government and defence and security forces, as well as various political parties and representatives.

The **National Observatory on Security Governance**, inaugurated in January 2017 was designed to act as a civil society think-tank for the control and monitoring of the security governance in Niger. A security official from the Ministry of Interior attended the organisation's launch. However, its actual input to the formulation of security and defence policies has been limited.

## Recommendations for civil society, academics, experts, media, and policymakers

1. Advocate for changes in the 2024 procurement law, to include provisions for disclosure of defence budgets and spending—initially in aggregated form, and subsequently in disaggregated form for non-sensitive expenditures, such as construction, vehicles, maintenance, general supplies, personnel, and pensions. Longer-term goals should include openness in non-sensitive areas of procurement.[104]

2. Advocate for the regular auditing of defence spending by the National Audit Office and the State Inspector General, even if it is not released to the public for several years. This would encourage additional oversight of defence expenditures in the absence of public access.

3. Engage with the government on issues of access to information, focusing on revising the ATI decree so that it includes balancing tests (harm and disclosure) and a maximum expiry time for classified information. A longer-term goal may include the enactment of a national law

4. Request official consultations on national security, with a minimum of being able to provide inputs to national security policies.
   a. Given the political climate, it may be more feasible to engage on security issues with subnational governments, such as at the level of regions, departments, or communes.

104 See the advocacy guide published by TI-DS in 2024 for an in-depth review of tactics and approaches to establishing access to information in the defence sector: Transparency International Defence & Security. "Defending Transparency: An Advocate's Guide to Counteracting Defence Corruption." London, 2024. https://ti-defence.org/publications/defence-security-sector-advocacy-toolkit-guide/.

CASE STUDY

# TUNISIA: ACCESS TO INFORMATION IN THE DEFENCE SECTOR

## Overview

1. Tunisia has faced intense democratic backsliding since the 2021 suspension of its constitution by current President Kais Saied, and the past few years have seen a decline in access to information across government.
2. Regardless, Tunisia has a strong access to information law, with an effective independent oversight body that has helped to implement the law throughout the public sector.
3. There are clear balancing tests specified in the law that require consideration of harm and public interest before withholding information, with implementing guidance, and the exceptions to disclosure are limited.
4. Since the events of 2021, the defence budget is released in aggregated form, while military spending has always been predominantly non-transparent. Defence procurement is primarily conducted offline rather than through the e-procurement platform, and weapons and armaments purchases are entirely confidential.
5. There have been no official consultations on national security in the last five years, and civil society organisations are blocked from engagement with government entities as a result of the current political climate.

## Country Context

With one of the strongest access to information laws in the world, Tunisia has had a formidable legal foundation for the exercise of the right to information since 2016.[105] The Access to Information Authority (Instance d'accès à l'information or INAI) was established shortly after the law was enacted, and in collaboration with other government departments, international partners, as well as civil society organisations, has succeeded in building a strong foundation for transparency within the public sector in less than a decade.

Despite the efforts of the INAI, defence-related information is often deemed confidential and not released to the public. This includes detailed budgets, expenditures, acquisition planning, and audit reports on defence matters by the major oversight agencies.

Tunisia has also faced intense democratic backsliding since the 2021 suspension of its constitution by current President Kais Saied, in which he also dissolved parliament. This was followed by the writing of a new constitution that consolidated power in the executive,[106] a new decree-law on cybercrime that has facilitated a crackdown on journalists and the media,[107] and a draft law in 2023 that would place civil society organisations under strict monitoring by the government.[108] In the midst of this turmoil, transparency and anticorruption efforts have been sidelined, and the armed forces

105 Global Right to Information Rating: https://www.rti-rating.org/country-data/

106 Grewal, Sharan, Salah-Dean Satouri, and Ian DeHaven. "Tunisia's New Constitution Will Only Worsen Its Political Crisis." Washington DC: Brookings Institution, July 6, 2022.

107 "Tunisian Authorities Escalate Clampdown on Media, Freedom of Expression." Amnesty International, May 30, 2024.

108 Benghazi, Lamine. "The Suffocation of Civil Society in Tunisia: A Chronicle of a Slow Constriction." *The Tahrir Institute for Middle East Policy.* November 9, 2023; "Tunisia: New Law Proposal Threatens Civic Space." Article 19, October 31, 2023.

have been increasingly enmeshed in the politics of the existing regime. The Access to Information Authority faces paralysis, with the retirement of its president, and an inability to reach quorum on decisions until the government appoints a replacement.

## RTI law and classification

Access to information in Tunisia enjoyed a period of institutionalisation throughout government for the five years following the enactment of the law establishing the right to information. However, since the dissolution of Parliament in 2021, civil society organisations have noted a dramatic drop in positive responses to public information requests. One organisation saw response rates drop from 93% in 2021 to less than 60% in 2022, highlighting the difficulties in accessing information during President Saied's tenure.[109]

The INAI has worked steadily to improve access to information in Tunisia, often in collaboration with civil society partners on trainings for public officials. It is also part of a global working group of independent high commissions for information, and works regularly with university and international development agencies to raise the profile of good practices in access to information.

**Table 17: Key features of ATI legal frameworks - Tunisia**

| | |
|---|---|
| **National legislation.** Any restriction on right to information must be present in the applicable national legislation. | Loi organique n. 22-2016 du 24 Mars 2016 relative au droit d'Access á l'information<br>Loi n° 88-95 du 2 Août 1988 relative aux archives. |
| **Exceptions related to defence.** The exceptions to the right of access based on national security are well-defined and consistent with international standards. | Art 24 of the 2016 ATI law states that disclosure may only be refused when this would cause harm to national security or defense, to related international relations, or to the rights of third parties with regard to the protection of their privacy, personal data and intellectual property. |
| **Harm test.** Information may be exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm. | Art 24 states that these areas are not considered absolute exceptions to the right of access to information. They are subject to the harm test provided that the harm is serious, whether concomitant or subsequent. |
| **Public Interest Test.** The law should provide for a public interest test when classified information is requested. | Art 24 notes that non-disclosure of these areas of information is also subject to the public interest test. Circulaire n° 2018-19 du 18 mai 2018, relative au droit d'accès à l'information provides instruction to public officials in balancing protected interests and the public interest when considering disclosure of information. |
| **Appeals.** Requesters have the right to lodge an appeal with an independent administrative oversight body. | The Access to Information Authority (INAI) plays a crucial role in adjudicating appeals on administrative denials. It is also responsible for monitoring and supporting implementation of the law across government. |
| **Declassification.** There should be a maximum expiry time in every secrecy regime. | Art 28 of the 2016 law states that classified information becomes accessible in accordance the law relating to archives. Per Art 16 of the 1988 law on archives, documents concerning national security cannot be declassified for 60 years.<br>However, concessions may be made for "scientific research" if there is no objection from the originating authority. |

109 Daïmi, Imad. "Fighting Tunisia's Rampant Corruption with Autocracy – Kais Saied's Chimera." *Just Security* (blog), November 22, 2022.

Kasbah, Tunis, Tunisia (Photo Credit: Brahim Guedich, Unsplash)

The INAI and civil society partners have been collaborating to draft a law on classification that would replace the various internal policies of ministries. In the interim, the law on archives has governed the classification of information, with a particularly lengthy confidentiality period of 60 years (see Table above).

With the exception of ATI requests involving potential harm to national security and defence, the Ministry of Defence (MoD) and Ministry of Interior (MoI) are the primary users of this exemption. However, other government agencies, such as the Central Bank and the High Judicial Council, have also cited this exemption in their refusal responses. In most instances, the INA has overturned the decisions of the MoD and MoI and has ordered both ministries to provide the requested information. However, no data is available on whether these reversal orders have been enforced.[110]

The ATI law also requires government agencies to proactively publish various types of information on their websites, such as procurement plans, audit reports, budget figures, and legal frameworks. In 2018, the MoD was the second least compliant ministry in meeting these proactive publishing obligations, just ahead of the Ministry of Justice.[111]

## Defence Finances

Since the 2021 actions by President Saied, Tunisia has scored poorly on budget transparency in the Open Budget Index. When the defence budget has been published in advance to the legislature and to the public for debate, it is in aggregate form, and failed to cover all aspects or describe detailed expenditures.

110 INAI annual reports 2021, 2020, 2019, and 2018
111 INAI Annual report 2018

Table 18: Open Budget Index scores among ATI case studies, International Budget Partnership 2023

| Country | Transparency Score (out of 100) | Rank (out of 125 countries) | % change since last index[112] |
|---|---|---|---|
| **Jordan** | 60 | 42 | -2% |
| **Egypt** | 49 | 63 | 14% |
| **Morocco** | 47 | 69 | -2% |
| **Saudi Arabia** | 26 | 98 | 13% |
| **Tunisia** | 16 | 104 | -62% |

Table 19: Military expenditures among ATI case studies, SIPRI 2023[113]

| Country | Military spending (USD millions) | % change 2022-2023 | % change 2014-2023 | Per capita spending | % of government spending |
|---|---|---|---|---|---|
| **Algeria** | 18264.0 | 100% | 88% | 400.5 | 19.34% |
| **Iran** | 10283.1 | 40% | 4% | 115.3 | 13.53% |
| **Kuwait** | 7755.0 | -6% | 33% | 1799.3 | 9.45% |
| **Morocco** | 5184.9 | 4% | 28% | 137.0 | 11.12% |
| **Tunisia** | 1208.2 | 4% | 33% | 97.0 | 7.05% |

Defence income from central government allocation is registered and shown in the budget, but information is not published in detail. The national service fund (funded by the contributions of conscripts and amounts paid by the structures for which services are rendered) is also included as a source of income, but it is primarily used for development projects in rural or remote areas. Otherwise, national defence institutions do not have beneficial ownership of commercial businesses, so there is no other source of defence income.

There is a lack of data available publicly on defence expenditure. Article 68 of the Budget Law specifies that annual performance reports (RAP) are annexed to the draft law on the settlement of the State budget for the budgetary year concerned. However, the budget settlement is often several years late to publication, and moreover, there is no legal requirement to make these reports publicly available. As a result, although the Ministry of Defence may prepare RAPs annually for internal purposes, they are rarely released to the public, as their publication remains at the Ministry's discretion.

THERE IS A
**LACK OF DATA**
AVAILABLE PUBLICLY ON DEFENCE EXPENDITURE

112 The +/- indicates whether the Transparency Score rose or fell against the last iteration of the Open Budget Index.

113 Average % of government spending: Middle East and North Africa: 12.78% (Saudi Arabia is highest at 24.04%)

## Defence Procurement

There is a formal decree that obliges the state to make public procurement available through the national procurement platform Tuneps (www.tuneps.tn). The portal provides the following services;

- **E-bidding:** includes the publication of tenders, receipt of offers and public opening of offers.
- **E-contracting:** where contracts between public buyers and winning bidders are drafted, modified, and signed, and in addition, evaluations, and statistical analyses are conducted.
- **E-product:** which features product registration, specifying characteristics, and nomenclature.
- **E-shopping mall:** a cyber market where public buyers may perform small value procurements directly from suppliers. This component caters mainly to small and medium enterprises (SMEs) that are financially unable to participate in large bids.

The requirement for online publication of tenders applies to the military, but at present, the MoD fails to use these tools, and many procurement cycles are not made public.

Purchases are usually published online before the actual purchases occur. However, other items such as munitions and armaments are treated with full confidentiality. Major defence purchases are often announced in the media, but information on confidential purchases (data on contracts, bidders, etc.) cannot be found through official publications.

## Transparency for Civic Engagement in defence matters

There have been no official consultations on national security in the last five years, and civil society organisations are blocked from engagement with government entities as a result of the current political climate. Information on defence matters is generally gleaned from the media or annual reports by oversight agencies, when available.

# THE REQUIREMENT FOR ONLINE PUBLICATION OF TENDERS APPLIES TO THE MILITARY

## BUT AT PRESENT, THE MOD FAILS TO USE THESE TOOLS, AND MANY PROCUREMENT CYCLES ARE NOT MADE PUBLIC

Table 20: Access to key documents related to defence matters - Tunisia

| Information | Public availability | Additional explanation |
|---|---|---|
| **Defence Strategy/Policy** | There is no defence strategy document. | Neither the parliament and executive have been able to produce a national security and defence strategy for Tunisia,[114] making it difficult to determine the long-term strategic direction of the armed forces. |
| **Audit reports** | Audits of the defence sector are produced by the Court of Auditors but not made publicly available. | Publicly available reports by the High Committee of Procurement may contain general information about the defence sector, but no details on contracts or suppliers. |
| **Asset Disposals** | Occasionally the Ministry of State Domains and Land Affairs holds open competition for tendering the disposal of assets, but it is not clear if this includes defence assets. | It is not clear whether the financial results of asset disposals are included as a source of income for the Ministry of Defence as there is no mechanism to make this information publicly available. |

114 DCAF. "Tunisia Country Strategy 2020-2024." DCAF Geneva Centre for Security Sector Governance, 2020.

# Recommendations for civil society, academics, experts, media and policymakers

1. Advocate for public disclosure of critical financial information about the defence sector, as outlined in the Tshwane Principles, including defence budgets, single source and competitive contracting, military acquisitions, defence income and foreign assistance, audit reports, disaggregated expenditures, and asset disposals.[115]

2. Call for the application of balancing tests for harm and public interest as specified in the access to information law to allow for the release of basic financial information (detailed budgets, income, and expenditures).

    a. Require the MoD to use the e-procurement platform Tuneps to release of information on tenders, awards, and contracts for non-armament purchases, asset disposals, as well as non-sensitive information on weapons and technological purchases.

    b. Continue collaborating with INAI on legal reforms for the classification of information, with attention to maximum expiry terms for classified information, and procedures for handling sensitive information across government departments and the national archives.

3. Advocate for official consultations on national security, with a minimum of being able to provide inputs to national security policies, and a focus on the production of a national security and defence strategy.

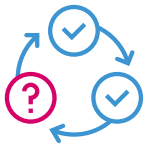
    a. Given the political climate, focus on facilitating consultations over security strategies with subnational governments—specifically at the level of governorate, district, and municipality.

115 See the advocacy guide published by TI-DS in 2024 for an in-depth review of tactics and approaches to establishing access to information in the defence sector: Transparency International Defence & Security. "Defending Transparency: An Advocate's Guide to Counteracting Defence Corruption." London, 2024. https://ti-defence.org/publications/defence-security-sector-advocacy-toolkit-guide/.

# SECTION 3

# CHALLENGES AND GOOD PRACTICES FOR ACCESS TO INFORMATION IN DEFENCE

## KEY INSIGHTS



A lack of capacity is often cited as the primary reason for failed implementation of access to information efforts. But bureaucratic failures are rarely that simple. Access to information presents challenges to cultures of hierarchy, secrecy, and risk aversion.

The absence of an administrative oversight body to assist with the implementation of right to information laws is a critical factor in whether access to information is fully realised across the public sector.

In the five case studies analysed in this report, the most common obstacle to effective access to information in the defence sector was the security classification scheme for information.

Balancing tests are critical for the appropriate withholding of sensitive information, as they require officials to weigh the benefit of disclosure against the potential harm to protected interests.

A means of countering the pressure to withhold information is the regular, proactive release of information that is recognised as being in the public interest, including a range of financial information, such as budgets, income, expenditures, oversight reports, and procurement.

Good practices for access to information pertaining to national security include consideration of exceptions to disclosure, length of classification period, administration and oversight, classification procedures, archival processes, and proactive release.

# Challenges to Access to Information

Access to information systems face an array of challenges that shift over the course of time, and are particularly vulnerable to changes in government, whether through elections or more violent actions such as coups or armed conflicts.

Democratic liberties and human rights are at risk in authoritarian regimes, where they are viewed as a threat to power. Due to their critical role in challenging power abuses and the improper exercise of authority, the right to information, along with freedom of expression and freedom of the press are often the first protections to be undermined or openly attacked in autocratic regimes. They are also threatened at other times of crisis, especially economic, military, or corruption-related, as shown in the cases in this report.

**Armenia** has seen high levels of defence spending because of its decades-long conflict with Azerbaijan over the Nagorno-Karabakh territory, which has recently concluded with major losses for Armenia. Access to information is enshrined in a national freedom of information law, but has been severely curtailed by the 2024 states secrets law, which prohibits the release of information related to most defence spending.

**Niger** experienced a military coup d'etat in July 2023 that has led to increased violence, stark reductions in foreign assistance, and a severe curtailing of access to information and other democratic rights. Even prior to the coup, defence income and military spending were mainly non-transparent, as were defence purchases. But a new far-reaching law was passed in 2024 that excludes all defence matters from public procurement, public accounting, and taxes.

**Guatemala** has endured a growing corruption crisis for the past decade, as the presidency and the Public Prosecutor's Office have stifled anti-corruption efforts, forced anti-corruption officials into exile, and blocked potential reform candidates from elections. As the Secretariat for Access to Public Information (SECAI) is required to work with the Prosecutor's Office on ATI enforcement, implementation of the law has faltered.

**Tunisia** has faced intense democratic backsliding and a decline in access to information across government since the 2021 suspension of its constitution. Still, Tunisia has a strong access to information law, with an effective independent oversight body that has helped to implement the law throughout the public sector.

**Malaysia** experienced its first peaceful transition of power in 2018 but, since then, has stalled on a number of governance reforms—including access to information. The Official Secrets Act 1972 (OSA) functions as the de facto national framework for access to information and overrules any other legislation on information access. There is little information about the defence budget or expenditures, and almost no publicly available information about acquisition planning.

# Key findings from case studies

In the five case studies analysed in this report, the most common obstacle to effective access to information in the defence sector was the security classification scheme for information. In Niger, the classification regime was overly broad, allowing nearly all information about the defence sector to be withheld from the public. In Armenia, prohibitions against disclosure were extremely specific, resulting in nearly all information about the defence sector being withheld. In Tunisia and Guatemala, national archives laws allow for prolonged or indefinite withholding of information, with little opportunity for access. In Malaysia, the lack of an access to information law has prevented the release of sensitive information to the public for the last several decades.

An issue critical to effective release of information in the defence sector is the presence of balancing tests in the law. These tests require officials to weigh the benefit of disclosure against the potential harm to protected interests.[116] This is often referred to as the "public interest test," and it is notably absent in three of the cases considered in this report (Armenia, Guatemala, Tunisia), with only Tunisia producing substantial guidance for public officials.

**Box 11: Categories of information with overriding interest in favour of disclosure, Tshwane Principles**

The Tshwane Principles outline the internationally agreed exceptions for national security and the categories of information with a high presumption or overriding interest in favour of disclosure, which should only be withheld on national security grounds in the most exceptional of circumstances and only for a strictly limited period of time. [117] This include:

A. Violations of international human rights and humanitarian law

B. Safeguards for the right to liberty and security of person, the prevention of torture and other ill-treatment and the right to life

C. Structures and powers of government

D. Decisions to use military force or acquire weapons of mass destruction

E. Legal framework and procedures for authorizing surveillance and use of collected material

F. Financial information

G. Accountability concerning constitutional and statutory violations and other abuses of power

H. Public health, public safety, or the environment

***In the five case studies analysed in this report, the most common obstacle to effective access to information in the defence sector was the security classification scheme for information.***

116 Lemieux, Victoria L., and Stephanie Trapnell. *Public Access to Information for Development: A Guide to Effective Implementation of Right to Information Laws.* Directions in Development. Washington, D.C.: World Bank, 2016.

117 Gross violations of human rights or serious violations of international humanitarian law may not be withheld under any circumstances. See Principle 10 of the Tshwane Principles.

**Table 21: Requirement to apply balancing tests in five country cases**

| | **Harm test.** Information may be exempted from disclosure if there is a real and substantial likelihood that its disclosure could cause serious harm | **Public Interest Test.** The law should provide for a public interest test when sensitive information is requested |
|---|---|---|
| **Armenia** | None. Based on absolute exceptions rather than a specific harm. | Only in a general sense: if the decline of the information request will have a negative influence on the implementation of state programs of the Republic of Armenia directed to socio-economic, scientific, spiritual and cultural development. |
| **Guatemala** | A harm test exists in the legislation. When a government agency seeks to categorize information as classified, the LAIP mandates fulfillment of three requirements:<br>1. The information falls under at least one of the defined reasons for classification.<br>2. Release of the information threatens an interest protected by the LAIP.<br>3. The damage or harm that may occur from publishing the information outweighs the public interest. | The public interest is considered as part of the harm test. |
| **Malaysia** | None. Based on absolute exceptions rather than a specific harm. | None. |
| **Niger** | None. Based on absolute exceptions rather than a specific harm. | None. |
| **Tunisia** | Restricted categories are not considered absolute exceptions to the right of access to information. They are subject to the harm test provided that the harm is serious, whether concomitant or subsequent. | Non-disclosure of information is also subject to the public interest test. *Circulaire n° 2018-19 du 18 mai 2018, relative au droit d'accès à l'information* provides instruction to public officials in balancing protected interests and the public interest when considering disclosure of information. |

Over the last few decades, it has become standard practice for governments to release financial information to the public on a regular basis. Defence exceptionalism has served to exclude the defence sector from this practice, with the argument that absolute secrecy is necessary for national security interests.

Implementing an access to information system within sectors that are circumscribed by extensive security classifications can be immensely difficult. It will encounter security exceptions when processing requests for information in sensitive areas. Balancing tests are a means of countering this obstacle as they require officials to weigh the harm of disclosure in a prescribed, legally mandated, and appropriate manner.[118]

118 The presence of an appeals body to consider whether balancing tests have been applied correctly is another key factor.

***Balancing tests are a means of countering excessive withholding of information, as they require officials to weigh the harm of disclosure in a prescribed, legally mandated, and appropriate manner.***

Another means of countering the pressure to withhold information is the regular, proactive release of information that is recognised as being in the public interest. When that is the case, specific kinds of disclosures are not triggered by information requests.

The Tshwane Principles acknowledge that information may be withheld from the public concerning the **details** of production, capabilities, or use of weapons systems and other military systems, including communications systems. But this should not extend to budget lines or expenditures concerning the **purchase or maintenance** of weapons and other military systems, as this information is necessary for evaluating and controlling the expenditure of public funds—including projected budgets, income, and expenditure information for authorities engaged in defence activities.[119]

**Documents that should be proactively released include:**[120]

1. Departmental and agency budgets;
2. End-of-year financial statements or expenditure reports;
3. Operational balance sheets and yearly financial statements for military-owned firms or enterprises, in areas such as pension management, weapons production, construction, natural resources, and development;
4. Financial management and procurement rules as well as control mechanisms;
5. Reports made by supreme audit institutions, procurement oversight committees, parliamentary committees, and other bodies responsible for reviewing financial aspects of the defence sector, including summaries of any sections of such reports that are classified;
6. Notifications of defence purchases and sales, including information on tenders, amounts, awards, suppliers, asset disposals, and significant contract modifications. This applies to both general services and major armament-related procurement;
7. The terms of concluded bilateral and multilateral agreements that concern security assistance (financing, sales, donations, grants, services, etc), and other major international commitments by the state on national security matters.

It is also good practice for states to report publicly a list of all arms exports and imports each year, which includes the types of weapons, the number of units and/or financial value for each weapon type, and the destination country, to fully respond to the ATT and the UN Register of Conventional Arms. States should also proactively publish information about weapons, equipment, and troop numbers.[121]

119 Tshwane Principles, 2013.
120 Government Defence Integrity Index, 2020.
121 Tshwane Principles, 2013.

### Box 12: List of proactively released information, mandated by law in Taiwan

In exploring best practices for access to information in the defence sector, we consider models that promote transparency and accountability while safeguarding national security. Effective practices include publicly accessible defence budgets, transparent procurement processes, and regular reporting on defence expenditures. Taiwan offers a valuable case study, with insights from Transparency International Taiwan highlighting its approach to open information.

Taiwan's equivalent to the Freedom of Information Act (FOIA) is the "Freedom of Government Information Law," which ensures that the public has the right to access government information. Under this law, several types of information are disclosed to the public, including:

1. **Government Budgets and Financial Reports**:
   - Detailed budgets, including the defense budget.
   - Financial reports and audits of government agencies.
2. **Policy and Decision-Making Information**:
   - Policies, plans, and regulations formulated by government agencies.
   - Minutes and resolutions from government meetings.
3. **Administrative and Operational Information:**
   - Organisational structures and responsibilities of government agencies.
   - Procedures and guidelines for administrative processes.
4. **Public Services Information:**
   - Information related to public services, including healthcare, education, and transportation.
   - Data on the performance and outcomes of public services.
5. **Statistics and Research Reports:**
   - Statistical data collected by government agencies.
   - Research reports and studies commissioned by the government.
6. **Environmental Information:**
   - Data on environmental quality, pollution, and conservation efforts.
   - Information on public health and safety related to the environment.

***Effective practices include publicly accessible defence budgets, transparent procurement processes, and regular reporting on defence expenditures.***

# Good Practices for Access to Information Pertaining to National Security

Balancing national security with public interest, the good practices below are being drawn from various countries to identify effective approaches to information access. By establishing transparent standards for public access and oversight, these examples demonstrate how defence institutions can build public trust and mitigate corruption risks.

**Exceptions:** Overly specific prohibitions on release of defence-related information and overly broad "blanket" prohibitions for national security purposes should be eliminated. They should be replaced by:

- Categories that align with the Tshwane Principles, and
- Balancing tests to determine whether withholding is appropriate on a case-by-case basis.

### Box 13: List of information withheld in the interest of national security, mandated by law in Taiwan

The Ministry of National Defense (MND) of Taiwan, like many defense organisations globally, withholds certain types of information from public disclosure to protect national security, operational integrity, and sensitive personal data. The specific types of information that are typically not disclosed include:

1. **Classified National Security Information:**
   - Details of military strategies, operational plans, and defense tactics.
   - Information on military capabilities, vulnerabilities, and readiness levels.
2. **Intelligence and Surveillance Data:**
   - Information obtained through intelligence operations.
   - Methods, sources, and details of surveillance activities.
3. **Technology and Weapons Systems:**
   - Technical specifications, designs, and capabilities of weapons systems and military technology.
   - Research and development information related to defense technologies.
4. **Operational and Deployment Information:**
   - Specific locations, movements, and statuses of military personnel and assets.
   - Details of ongoing or planned military operations and exercises.
5. **Security and Counter-Terrorism Measures:**
   - Information on counter-terrorism strategies and operations.
   - Details of security measures in place to protect critical infrastructure and key assets.
6. **Confidential Communications:**
   - Internal communications and deliberations within the MND and with other government agencies.
   - Diplomatic communications related to defense and security matters.
7. **Personal Data and Privacy:**
   - Personal information of military personnel and their families.
   - Health records and other sensitive personal data.
8. **Agreements and Contracts with Defense Contractors:**
   - Certain details of defense procurement contracts, especially those containing proprietary or classified information.

**Length of classification:** Information should be withheld on national security grounds for only as long as necessary to protect a legitimate national security interest.

- The withholding of information needs to be moderated by maximum expiry times for classified information. No information may remain classified indefinitely.
- Decisions to withhold information should be reviewed every 5-10 years to ensure that withholding is still appropriate.

***An access request can be made for any record under the control of an institution, regardless of its security categorisation.***

### Box 14: Declassification in Canada's access to information regime

Canada issued instructions for declassification in *Access to Information Implementation Notice 2023-02: Leveraging Access to Information to Promote Declassification and Downgrading of Government Records:*

Government officials assign a security category (classified or protected) to records based on the degree of injury associated with the record being disclosed. These categories range from risks to an individual's privacy and personal dignity to those related to Canada's national interests and security. Security categorisation is based on the risks that exist at the time they were applied and dictate how government officials handle and store the information.

An access request can be made for any record under the control of an institution, regardless of its security categorisation. A decision to deny access to a record, or any part of it, must be based solely on the exemption or exclusion provisions of the *Access to Information Act* as they apply at the time of the request. A decision to deny access must not be based on security categorisation, however recently it may have been assigned.

Classified or protected information may lose its sensitivity with the passage of time or after the occurrence of specific events. When it is determined that the expected injury of disclosing such information is reduced, the original record should be considered for declassification or downgrading.

**Administration and Oversight:** Implementation of access to information frameworks requires two types of administration:

- Trained and qualified personnel in ministries to handle information requests, who are familiar with the legal rules around withholding of information and can provide justifications for refusals that correspond to those legal rules.
- An independent administrative oversight body with the capacity to handle secondary appeals and to issue clarifying opinions for withholding and release.[122] The oversight body should also have the authority to train personnel and oversee implementation, and to enforce the access to information framework through both penalties and support to agencies.

122 For further discussion of ATI independent oversight bodies, see Banisar, David. "Shining the Light on Corruption: Freedom of Information and Transparency in Central and Eastern Europe." CEELI Institute. October 2024.

### Box 15: Functions of oversight bodies in United States

Oversight of access to information in the United States is performed by two separate units:

1. The mission of the Office of Information Policy (OIP) is to encourage and oversee agency compliance with the Freedom of Information Act (FOIA). It is based in the Department of Justice.

    - **Guidance:** OIP is responsible for developing government-wide policy guidance on all aspects of FOIA administration.
    - **Training:** OIP provides legal counsel and training to agency personnel.
    - **Legal advice:** To assist agencies in understanding the many substantive and procedural requirements of the FOIA, OIP publishes a comprehensive legal treatise addressing all aspects of the FOIA. OIP also provides a range of resources to agencies to guide them in their administration of the Act.
    - **Compliance:** In addition to its policy functions, OIP oversees agency compliance with the FOIA. All agencies are required by law to report to the Department of Justice each year on their FOIA compliance through submission of Annual FOIA Reports and Chief FOIA Officer Reports. OIP develops guidelines for those reports, issues guidance and provides training to agencies to help them complete the reports.
    - **Reporting:** The OIP reviews and compiles summaries and assessments of agency progress in administering the law.

2. The Office of Government Information Services (OGIS) is a Freedom of Information Act (FOIA) resource for the public and the government. It is based in the National Archives.

    - **Policy review:** The OGIS reviews FOIA policies, procedures, and compliance of federal agencies and identifyies ways to improve compliance.
    - **Ombudsman:** The mission of the OGIS also includes resolving FOIA disputes between federal agencies and requesters.

**Classification procedures:** Procedures and standards governing classification should be publicly available, and the public should have the opportunity to provide inputs on the procedures and standards governing classification.

**Archives:** Information should be managed and maintained by governmental authorities according to international standards. National archives institutions should coordinate with governmental agencies to ensure appropriate preservation of documents.

**Proactive release:** Certain categories of information related to defence should be regularly released to the public without need for an information request to trigger release, including information on finances, procurement, and administrative structures.


## Accountability Ecosystems

A growing body of research reveals that a lack of access to information cripples civilian oversight of the defence sector.[123] Ongoing and excessive secrecy *within* government contributes to the failure to review defence policies and budgets, conduct investigations, and issue recommendations. Inter-institutional accountability mechanisms, such as those conducted by parliaments, inspectors general, supreme audit institutions, and procurement bodies, are unable to monitor performance or adherence to rules and regulations. The absence of *publicly* available information denies civil society organisations access to fundamental aspects of defence policymaking and finances that are inherently part of the vertical process of democratic accountability. This lack of transparency carries severe consequences for the defence sector: it obstructs civic engagement in defence matters, impedes institutional accountability, and threatens the legitimacy of the defence establishment.

Transparency, oversight, and civic space form the foundation for effective democratic governance of the defence sector, and by extension, serve as factors in mitigating corruption risk. Robust civic space, and freedom of expression in particular, are critical prerequisites for democracy, and serve as safeguards against war and conflict.[124] While individually, these elements may lack the force to transform weak governance or neutralise corruption risks, together they constitute an *ecosystem of accountability* of many interconnected and dynamic components, encompassing both the individual and institutional. Accountability ecosystems involve multiple relationships and levels of government, civil society advocacy, and institutional cooperation, with the understanding that power plays an important role in both the problem and the solution.[125]

> ***Robust civic space, and freedom of expression in particular, are critical prerequisites for democracy, and serve as safeguards against war and conflict.***

123 Goodman, Colby. "Blissfully Blind: The New US Push for Defence Industrial Collaboration with Partner Countries and Its Corruption Risks." Transparency International Defence & Security, 2024; "Trojan Horse Tactics: Unmasking the Imperative for Transparency in Military Spending." Transparency International Defence & Security. 2024; Picard, Michael, and Colby Goodman. "Hidden Costs: US Private Military and Security Companies and the Risks of Corruption and Conflict." Transparency International Defence & Security, 2022; "GDI 2020 Global Report: Disruption, Democracy, and Corruption Risk in Defence Sectors." Transparency International Defence & Security. 2021; "The Missing Element: Addressing Corruption through Security Sector Reform in West Africa." Transparency International Defence & Security, 2021; "Defence Industry Influence on European Policy Analysis: Findings from Italy and Germany." Transparency International Defence & Security, 2021; "Progress [Un]Made: Defence Governance in Central and Eastern Europe." Transparency International Defence & Security, 2020.

124 "Betrayed by the Guardians: The Human Toll of Corruption in Defence and Security." Transparency International Defence & Security, 2024.

125 Halloran, Brendan. "Strengthening Accountability Ecosystems: A Discussion Paper." Transparency & Accountability Initiative, 2015.

***Transparency, oversight, and civic space form the foundation for effective democratic governance of the defence sector, and by extension, serve as factors in mitigating corruption risk.***

In other words, transparency, which includes access to information, is necessary but not sufficient for consequential governance outcomes. Indeed, it is not just a *transparency* or *accountability* or *participation* problem. Weak accountability, a lack of transparency, or shrinking civic space all exist within a complex system of governance, where failures will require a combination of contextually adapted or designed reforms. Effective access to information, combined with a system of robust oversight (including by civilian actors), meaningful civil society engagement, and a commitment to openness and integrity, are therefore critical components in managing corruption risks within the defence sector.

Finally, the challenge of establishing access to information in the defence sector is reflected in the ongoing difficulties identified in all of the case studies undertaken. Rather than simply a case of a weak legal framework or lacklustre implementation, all of the cases reflect complex issues that are intertwined and thus not easily solvable. Yet all of but one of them have access to information frameworks that function to some extent. This is a result of the political and bureaucratic foundations laid by advocates both in and outside government, during periods of support from governments in power at that time. Moreover, all of the cases benefit from strong civil society advocacy for openness and transparency, which endures even in the face of rising authoritarian power, military coups, and regressive tendencies in policymaking.

Military helicopters (Photo Credit: Juli Kosolapova, Unsplash)

Transparency International Defence & Security
10 Queen Street Place
London
EC4R 1BE

ti-defence.org
twitter.com/@TI_Defence

Transparency International UK
Registered charity number 1112842
Company number 2903386