TRANSPARENCY INTERNATIONAL
Defence & Security

WATCH
ORGANISATION

FROM TEXT TO PRACTICE

Applying Tunisia's Access to Information Law to 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 worldwide.

I WATCH is a Tunisian watchdog organisation founded in 2011 aiming at fighting corruption and enhancing transparency. In 2013, I WATCH became the official contact point of Transparency International in Tunisia, and since 2017 it has been a 'Chapter in Formation' of Transparency International.

Published January 2019.

Transparency International UK's registered charity number is 1112842.

FROM TEXT TO PRACTICE:

Applying Tunisia's Access to Information Law to Defence

1. INTRODUCTION/ EXECUTIVE SUMMARY

Following several years of debate, Tunisia finally has strong legislation regarding access to information. The government adopted a law to this effect in 2016, praised by many as being one of the most progressive access to information laws in the world. However, the law has faced limitations to its application, which include overzealous application of national security related exceptions.

Transparency International Defence & Security and I WATCH (Transparency International's national chapter in Tunisia) have conducted research to understand how the access to information law is being implemented in the defence sector. We have spoken with Members of Parliament, independent commissions and civil society organisations (CSO) in Tunisia, and conducted desk research. Additionally, I WATCH has filed several access to information requests to the MOD directly, to evaluate the nature of responses received. These activities have provided the findings, and formed the basis of our conclusions and recommendations, outlined below.

National security remains a priority for Tunisia's government. Defence and security forces face numerous challenges, and the country has been in a state of emergency since November 2015, following three major terrorist attacks that year. Despite this, another attack was committed in Tunis in October 2018, apparently targeting security forces and reiterating the urgency of confronting terrorist threats in Tunisia.[1] While national security is key to achieve military objectives and strategies, it is important to ensure that the MOD does not overwhelmingly use it as an excessive justification to obscure access to information. Achieving the appropriate balance between legitimate national security concerns and the public's right to access information has been a recurring challenge, and we have found that attitudes of secrecy currently prevail over good practice, in particular within the defence sector. Access to information legislation, while strongly worded, has been sparsely and ineffectively applied, and the MOD in particular has often justified its refusal to provide responses to access to information requests based on national security or lack of capacity.

2. ORIGINS AND EARLY APPLICATION OF THE LEGISLATION

Upon its adoption in 2016, civil society and international non governmental organisations (NGOs) hailed Tunisia's access to information law as one of the most progressive pieces of legislation on access to information worldwide, designed to empower Tunisian citizens and civil society to access information and improve government transparency and accountability.[2] The law guarantees the right to access information by requiring that government bodies answer requests for information in a timely manner. Importantly, it emphasises that access to information includes both the publication of information on request, as well as the proactive publication of information by the concerned bodies.[3] Certain exceptions to this right exist.

Exceptions to the right to request information

Citizens and private persons can request any information from government agencies, provided this information does not fall under exceptions outlined in article 24. According to this article, a public body can reject a request, which might result in prejudice to national security or defence, to international relations related to these, or to third party rights such as to the protection of private life, personal data, and intellectual property.

Importantly, there is a caveat to these exceptions. Article 26 adds, "The fields listed are not considered as absolute exceptions to the right to information and shall be subject to a prejudice test. The damage shall be substantial and encompass current and future damage."[4] The onus lies on the public body in question to justify any refusal to provide information, and the law provides appeals processes through the newly created Access to Information Authority (INAI), and through administrative tribunals, if the person requesting information is unsatisfied with the public body's response.[5] The final version of this article resulted from online and lobbying campaigns led by CSOs including I WATCH and Al Bawsala putting pressure on Parliament to withdraw the first version, which presented a real threat to the applicability of the law by providing a long list of possible exceptions from which government authorities

1 "Tunisie: une femme s'est faite exploser sur l'avenue Bourguiba dans le centre ville de Tunis, plusieurs blessés," AFP/HuffPost (web), October 29, 2018

2 Loi organique n°2016-22 du 22 mars 2016, relative au droit d'accès à l'information: www.legislation.tn/fr/detailtexte/Loi-num-2016-22-du-24-03-2016-jort-2016-026__2016026000221?shorten=TgGW. Tunisian legislators adopted the law on March 22, 2016, and it came into force in March 2017. It superseded Law-Decree n°41-2011, the first piece of legislation regarding access to information in Tunisia, and allowed Tunisia to meet the requirements of the Open Government Partnership (OGP) which it had joined in 2014.

3 Loi organique n°2016-22 du 22 mars 2016, Art. 3

4 "Tunisia Assembly Adopts Freedom of Information Law", Freedominfo.org (web), 14 March 2016: http://www.freedominfo.org/2016/03/tunisia-assembly-adopts-freedom-of-information-law/

5 Loi organique n°2016-22 du 22 mars 2016, Art. 29-31

could choose to restrict information.[6]

The INAI has at times rejected the national security exception with article 26. In one case, a journalist had sent a request to the Ministry of Interior in July 2018, asking for statistics related to the number of persons subject to a specific border control measure ("Procedure S17"), and their geographical distribution. When the ministry did not respond, the journalist filed a claim to the INAI, who asked the ministry to justify the rejection of the request; the ministry answered in September 2018 quoting article 24 on the grounds of personal data protection and of national security, because the procedure aims to identify and control suspects of terrorism or other infractions.[7] However, the INAI rejected this argument, noting that the request was specific to statistics, not personal data—therefore, under article 26, the ministry did not justify the potential harm, and the INAI ruled that the journalist should be allowed to access the statistics to help enhance transparency and accountability towards the management of security bodies.[8]

Certain, but uneven, progress

Imed Hazgui, president of the INAI, notes that there has been progress towards the implementation of the access to information legislation. The commission is up and running, with members in place and claims being submitted. In November 2018, the INAI formally launched their website, which includes information about the authority, procedures relating to access to information, and decisions that have been adopted.

However, despite some positive steps on paper, there remain limits to the law's effective application,[9] which the authority and the government should aim to address. For instance, as of November 2018, citizens and CSOs had filed 505 claims with the INAI regarding access to information; of these, 304 were still pending.[10] While the number of claims indicates the public's willingness to access information, the number of pending responses demonstrates institutional limits to respond. While the commission's creation has reinforced the legitimacy to exercise the right to access information, the government must demonstrate further political will and commitment by adopting clarifying texts and speeding up access to information. Hazgui suggests, for example, giving the INAI the power to hire its own agents as opposed to having them appointed by the head of government, to "consecrate" the access to information "culture."[11]

I WATCH has found that responsiveness towards access to information requests has increased compared to the previous law, but some government bodies remain resistant to releasing information. As such, they have often ignored deadlines for responses, and used unrealistic arguments to justify rejecting requests or referring them to courts, where they may remain caught for extended periods. I WATCH demonstrated in September 2018 that only five of the 26 ministries fully respect article 6 of the law, about proactive publication of information; most of the other ministries have not updated their websites to include reports and documents that they should have been proactively sharing.[12] Between January and August 2018, I WATCH submitted 193 requests for information. 73 were related to corruption cases and investigated by I WATCH's Advocacy and Legal Advice Centre (YALAC), and 120 were submitted as part of the oversight process. I WATCH appealed over 50% of the requests to the INAI, either for ignoring the requests or for rejecting them.

Another hurdle identified by I WATCH is the lack of training and understanding of the law from Access to Information officers within the government, who are supposed to implement the law's provisions and respond to queries. From I WATCH's experience and interviews, including with the INAI, there is a sense that due to limited training, administrative employees have at times wrongly rejected requests based on data protection, or other exceptions, and have demonstrated limited understanding on how to test the exceptions under article 24. I WATCH also acknowledge the challenge posed by the lack of digitalisation across the Tunisian public administrations, making the process of producing the necessary documents to respond to access to information requests slow and laborious and meaning that non-compliance with deadlines may sometimes simply be due to the time it takes to do so. One interviewee from a public oversight body suggests focusing on strengthening administrative employees' capacity through collaborative programs between the INAI, CSOs, and public institutions. This would for instance help dissipate legitimate concerns about the limits of personal data or national security, and ensure that ministries use these exceptions in adequate circumstances, rather than as a defence in general scenarios and benign requests.

6 T. Dreisbach, "Information for the People: Tunisia Embraces Open Government, 2011-2016," Princeton University (web), May 2017: https://successfulsocieties.princeton.edu/publications/information-people-tunisia-embraces-open-government; see also Aymen Gharbi, "Tunisie: Le projet de loi organique sur le droit d'accès à l'information "contraire à la constitution", selon deux associations," HuffPost Maghreb (web), 13 March 2016: https://www.huffpostmaghreb.com/2016/03/09/tunisie-acces-information_n_9416824.html

7 "'S17' Victims of the Ministry of Interior's Whims," Arab Reporters for Investigative Justice, 24 November 2018: https://en.arij.net/report/s17-victims-of-the-ministry-of-interiors-whim

8 The full decision, dated 4 October 2018, is available on the website of the INAI: http://www.inai.tn/plaintes_avis/%D9%82%D8%B1%D8%A7%D8%B1-%D8%B9%D8%AF%D8%AF-251-%D8%A8%D8%AA%D8%A7%D8%B1%D9%8A%D8%AE-2018-10-04/ There have been reports that the Ministry of Interior has appealed the decision.

9 K. Ferchichi, "Quand l'application de la loi fait défaut," La Presse (web), September 2018, available at: https://www.turess.com/fr/lapresse/153598

10 "Tunisie : 505 plaintes déposées auprès de l'instance d'accès à l'information," Webmanagercenter (web), November 2018: https://www.webmanagercenter.com/2018/11/27/427536/tunisie-505-plaintes-deposee-aupres-de-linstance-dacces-a-linformation/

11 Ibid.

12 "Management Guide to Access to Information," I WATCH, 5 October 2018: https://www.iwatch.tn/ar/article/625

3. UNEQUAL APPLICATION OF THE LEGISLATION IN THE DEFENCE SECTOR

The MOD has had some good practices and engagements with the access to information authority, for instance being one of the first ministries to send their annual report on access to information. The ministry outlines contact information of those responsible for access to information requests, and procedures to undertake.[13] According to their website, dedicated personnel within the ministry receive and respond to ATI requests. In 2017, the MOD received 22 requests and answered all of them: two were sent to the national centre for cartography and remote sensing, and 17 to the office of military housing. There still exist some challenges however; as of publication, 13 claims against the MOD are pending before the Access to Information Authority.[14]

Requests for Information

Few studies or initiatives have analysed the transparency of the MOD and its adherence to the new legislation until now. I WATCH have sent several access to information requests to the MOD, and have found that the ministry has responded to most of them within the 20 day limit imposed by the law. The issue lies within the content of the answers, with responses using the exemptions of article 24 regarding national security or claiming that they cannot disclose the information due to lack of human and technical resources.

Ostensibly, the defence sector–represented largely by the MOD–is the same as any other public sector in terms of its legal obligation to comply with the access to information legislation. Like any other public administration, the MOD must adhere to regulations and processes governing the legislation, and can only refuse to grant access to a piece of information in the exceptional circumstances provided for in article 24.

However, the MOD have often relied on the national security defence as a way to avoid giving detailed responses to access to information requests. While the ministry has a good record of responding to requests, they have often explained that they cannot provide information due to the national security imperative. While the law requires that ministries or public authorities justify their refusal to provide information under article 24, ministries utilise the exceptions as the justification itself without necessarily elaborating as to why they are invoking them. This creates a vacuum in which the ministry may provide an apparent explanation, but one devoid of sense or transparency to the requesting party.

National security concerns are naturally higher in the defence sector than in most others, but it is crucial to balance national security with the public interest if the defence sector is to retain public trust. The law requires that decision-makers evaluate this balance, which is crucial to ensure accountability and to ensure that the public understands and identifies corruption risks and can act as a check. With legislation on this matter already in place, it is for the Ministry to adopt a clear and transparent classification framework to guide how information is classified and how requests for information are responded to. The Parliament or the INAI should support this endeavour by adopting a clear definition of 'national security' which public administrations including the Ministry of Defence should refer to in their classification guidelines.

Proactive Publication of Information

From a public information standpoint, the Ministry of Defence website, like that of other ministries, lacks published information, notably its strategy for operations, financial reports, on its procurement procedures, on its military and non-military acquisitions, and on updates regarding the access to information law such as proactive publication of auditing reports and statistics reports related to services and operations. Some information is outdated, such as the information regarding deployment and participation in United Nations peacekeeping operations, and could be updated without obvious risks to national security.[15]

13 "Accès à l'information," République Tunisienne, Ministère de la Défense Nationale: http://www.defense.tn/index.php/fr/acces-aux-documents-administratifs

14 "Tunisie : 505 plaintes déposées auprès de l'instance d'accès à l'information," Webmanagercenter (web), November 2018: https://www.webmanagercenter.com/2018/11/27/427536/tunisie-505-plaintes-deposee-aupres-de-linstance-dacces-a-linformation/

15 The section of the Ministry of Defence website dedicated to peacekeeping operations includes a graph with the ongoing and past peacekeeping operations that the Tunisian government has been a troop contributing country to. Among these, the United Nations Operation in Cote d'Ivoire (UNOCI) is listed as ongoing, despite the operation having completed its mandate in 2017. See: http://www.defense.tn/index.php/fr/missions-de-l-onu

Applying Legislation to Tunisia's Defence Sector: I WATCH Access to Information Requests

I WATCH have been testing the legislation to ensure its correct application since the law's adoption in 2016. In order to get a clearer picture of how the MOD in particular is responding to access to information requests, IWATCH has filed several access to information requests with the MOD, outlined below.

The first request submitted to the MoD relates to the number of civilians prosecuted by military courts.[16] The Tunisian military has on multiple occasions tried and convicted civilians accused of being critical of the military, without there being any public records on the number of cases involved. I WATCH asked the MOD to release the number of cases; the Ministry responded that they could not release the information because they do not have the resources to collect this data.

The MOD rejected another two ATI requests made by I WATCH based on article 24's exceptions regime in the name of national security. One of these concerns public procurement: I WATCH requested information on the number of public procurement contracts and the names of suppliers: "1. the list of suppliers contracted by the Ministry of Defence to provide equipment, supplies, or services (contracts of 50,000 dinar or over) during the year 2017" and "2. the number of contracts with each of these suppliers."

The second asks for "the number of meetings between members of the MOD and members of the Parliamentary Defence and Security Committee during 2017 and the beginning of 2018, and minutes from these meetings." This committee monitors security and defence related issues in Tunisia, including through meetings and hearings with government security officials to implement national security policies and hold them accountable to reforms. I WATCH submitted both of these requests on 14 August 2018, and the MOD answered within 10 days—fully respecting the 20-day deadline imposed by the law.

In the absence of any justification of the usage of the national security exemption or public availability of any guidelines that officials followed in order to reach this conclusion, it is unclear how or why the MOD judged that the danger to national security in releasing these pieces of information outweighed the public interest and decided to apply Article 24 in these cases.

16 Human Rights Watch, 2018

4. INTERNATIONAL BEST PRACTICES REGARDING ACCESS TO INFORMATION IN THE DEFENCE SECTOR

Accessing information in the defence sector can be complex, due to the importance of balancing the right of the public to follow up on the performance of their government with legitimate secrecy regarding specific national security and public order issues. Legislators worldwide have attempted to tackle the national security dilemma with regards to access to information, and imposed restrictions and strict classification rules to areas where government secrecy is legitimate, leading to a body of best practices and recommended tests to determine legitimate exceptions. As such, many freedom of information acts or right to information acts, have developed procedures outlining the exceptions regime, and appeal mechanisms with external bodies such as courts and independent commissions if they are dissatisfied by the government's response or application of an exception.[17]

The Tshwane Principles: A Step towards Clearer Legislation

In 2013, the Tshwane Principles on National Security and the Right to Information set out "unprecedented guidelines for those engaged in drafting, revising, or implementing laws or provisions relating to the state's authority to withhold information on national security grounds or to punish the disclosure of such information."[18] These principles primarily cover the relationship between "national security and freedom of expression, whistle-blower's protection, oversight bodies, and judicial oversight."[19] According to the Tshwane Principles and a growing number of international texts relating to the right of access to information, exceptions must be proportionate and necessary.

Limiting Exceptions to Access to Information

When information must be restricted, the Tshwane Principles note that governments should make the restrictions clear in law, and must be in order to protect a legitimate national security interest.[20] In terms of access to information in the defence sector, states such as New Zealand, the United Kingdom, or the United States, demonstrate their interest in transparency by dedicating sections of their legislations to the disclosure of MOD files and reports, as well as outlining procedures and answers to access to information requests within government agencies.[21] Additionally, the Tshwane Principles are clear that public authorities must provide "specific, substantive reasons" to support the application of restrictions, and several tests can determine the limits to the exceptions regime.[22]

The so-called **"harm test"** requires that a public authority demonstrate that the disclosure of certain types of information will cause harm to a protected interest. The state must prove that the disclosure of information would cause substantial and demonstrable harm to a legitimate interest. Importantly, the harm cannot be speculative or remote, and must instead by sufficiently specific, concrete, imminent, and direct.[23]

On the other hand, the **"public interest balancing test"** requires consideration of proportionality of the harm caused against the public interest. It requires that the oversight body or public authority weigh the harm that disclosure would cause to a certain protected interest, against the harm that could occur from disclosure of the

17 "Open Development: Access to Information and the Sustainable Development Goals," Article 19 (web), 19 July 2017: https://www.article19.org/resources/open-development-access-to-information-and-the-sustainable-development-goals/

18 "Understanding the Tshwane Principles," Open Society Justice Initiative (web), 12 June 2013: https://www.opensocietyfoundations.org/briefing-papers/understanding-tshwane-principles

19 "Classified Information: A review of current legislation across 15 countries & the EU," TI-DS (web), 2014:12: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

20 The Global Principles on National Security and the Right to Information, 2013: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

21 See, for example, "How to make a freedom of information (FOI) request," UK Government, https://www.gov.uk/make-a-freedom-of-information-request; "How do I make a FOIA request?" https://www.foia.gov/how-to.html; Official Information Act Requests, New Zealand Ministry of Defence, https://www.defence.govt.nz/about-this-site/oias/

22 The Global Principles on National Security and the Right to Information, Principle 4, 2013: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

23 "Balancing Openness and Confidentiality in the Defence Sector: Lessons from International Good Practice," Centre for Integrity in the Defence Sector (web), 5 June 2018: 11: https://cids.no/2018/06/05/new-guide-to-good-governance-on-openness-and-confidentiality-in-the-defence-sector/

information.[24] The Tshwane Principles rely on government bodies ensuring that disclosure of information poses a real and identifiable risk of "significant harm," which must "outweigh the overall public interest in disclosure." At the same time, the restriction must comply with the principle of proportionality, be the least restrictive means to protect against harm, and "must not impair the very essence of the right to information."[25] Countries including the United Kingdom and Australia apply this principle, and Tunisia has codified this test into Article 24 of the 2016 law.[26]

Facilitating Access to Information Requests

As discussed above, public bodies are required to facilitate access to information, and respond to requests from the public, as recommended by the Tshwane Principles; in Tunisia, this is codified in the 2016 law and the Tunisian MOD's procedural handbook specifies that access to information includes the right to access information on request.[27] Several countries have adopted good practices in this regard, by appointing additional staff and clarifying the procedures and the limits within which limits officials may refuse to respond to requests. In Tunisia, the Access to Information Law codifies these procedures and the MOD procedures manual specifies whom to contact within the Ministry.[28]

Freedom of information requests in the UK have prompted the MOD to publish further financial and human resources information such as quarterly service personnel statistics,[29] senior staff salaries,[30] and business plans.[31] The UK MOD also proactively publishes reports from FOI requests on a weekly to biweekly basis, making responses to FOI requests easily accessible.[32]

The US Department of Defence (DOD), on the other hand, makes freedom of information requests easy to conduct, by publishing details on the procedure and the 1966 Freedom of Information Act (FOIA) legislation online.[33] The department publishes annual reports on FOIA requests online; these show the progress achieved since the law's implementation.[34] Additionally, the DOD specifies, "Federal agencies are required to disclose records upon receiving a written request for them, except for those records that are protected from disclosure by any of the nine exemptions or three exclusions of the FOIA. This right of access is enforceable in court."[35] When the department refuses to disclose information, it is required to provide an in-depth justification to explain the rationale behind the refusal, and the way in which disclosure may affect national security more adversely than it would serve a public interest.

These examples demonstrate some key considerations that governments should take into account when determining whether to release information. Additionally, the law should set out clear criteria for classification and declassification, including ensuring time limits, conditions under which information should be declassified, and authorities responsible for declassification.[36] This provides an additional limit to governments' ability to restrict information, and may help prevent agencies from applying their own self-interest or overly classifying information.[37]

Proactive Publication of Information

As part of the right to access information, governments should also proactively publish information on their websites. This requirement extends to ministries of defence of these countries, and there are multiple examples of defence ministries publishing information with a varying degree of transparency, to enable citizens to comprehend their strategy and overarching goals. In Tunisia, the MOD procedural handbook specifies that access to information includes proactive publication of information by concerned bodies.[38]

Both the New Zealand and the UK governments

24 Ibid.

25 The Global Principles on National Security and the Right to Information, Principle 3, 2013

26 "Ministry of Defence Access to Information Guidance Note," UK Ministry of Defence, June 2009: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/16835/E420090701MOD_FOI_Guidance_Note.pdf; "FOI fact sheet 8: Freedom of information – Exemptions," Australian Government, Office of the Australian Information Officer: https://www.oaic.gov.au/freedom-of-information/foi-resources/foi-fact-sheets/foi-fact-sheet-8-exemptions; Loi organique n°2016-22 du 22 mars 2016, Article 24.

27 République Tunisienne, Ministère de la Défense Nationale, "Manuel de procédure pour l'accès à l'information," http://www.defense.tn/images/PDF/acces-info-FR.pdf; Loi organique n°2016-22 du 22 mars 2016, Chapitre 3.

28 Ibid.

29 "National Statistics: Quarterly service personnel statistics: 2018," Ministry of Defence, 15 February 2018: https://www.gov.uk/government/statistics/quarterly-service-personnel-statistics-2018

30 "Transparency data: MOD roles and salaries: 2017," Ministry of Defence, 25 January 2018: https://www.gov.uk/government/publications/mod-roles-and-salaries-2017

31 "Corporate report: Ministry of Defence single departmental plan," Ministry of Defence, 23 May 2018: https://www.gov.uk/government/publications/ministry-of-defence-single-departmental-plan/ministry-of-defence-single-departmental-plan-may-2018

32 "Publications: FOI releases," UK Ministry of Defence: https://bit.ly/2AM7i61

33 "Freedom of Information Act: Department of Defense Open Government," US Department of Defense: https://open.defense.gov/Transparency/FOIA.aspx

34 "Department of Defense Annual FOIA Report to the Attorney General," DOD Open Government, US Department of Defense: https://open.defense.gov/Transparency/FOIA/DoD-Annual-Reports-to-AG/

35 "Freedom of Information Act: Department of Defense Open Government," US Department of Defense

36 The Global Principles on National Security and the Right to Information, Principle 17, 2013

37 Centre for Integrity in the Defence Sector, June 2018: 12

38 République Tunisienne, Ministère de la Défense Nationale, "Manuel de procédure pour l'accès à l'information," http://www.defense.tn/images/PDF/acces-info-FR.pdf

proactively publish information on their websites, for instance. New Zealand's government discloses a large number of documents on topics ranging from the chief executive's expenses, MOD strategies, annual reports, to strategic defence policy review documents.[39] Their website also contains provisions regarding the New Zealand Defence Forces' engagement with the defence industry, publishing for instance the criteria that the ministry evaluates before making a deal with a defence company.

The UK MOD also publishes wide-ranging information proactively, with an Open Data Strategy designed to help it achieve its targets. Much of the information is released proactively and can be accessed through the MOD website, for instance financial information relating to projected and actual income and expenditure, tendering, procurement and contracts. This also includes documents outlining allowance changes, finances, gifts, hospitality, travel, and meetings received by ministers, gifts and hospitality received by senior officers and special advisers. The MOD website also contains information on the ministry's relationship with the defence industry, for instance publishing a 2016-2026 timeline of the procurement contracts the ministry intends to complete.[40] The same website includes details of defence contracts, including the number of jobs created within the MOD and the estimated amount the defence sector costs taxpayers per capita, ensuring transparency and clarity for the public.

39 See "Publications," New Zealand Ministry of Defence: https://www.defence.govt.nz/publications/

40 "A Breakdown of Planned Defence Expenditure 2018," Defence Contracts Online: https://www.contracts.mod.uk/blog/breakdown-planned-defence-expenditure-2018/

5. CONCLUSIONS AND RECOMMENDATIONS

Guaranteeing transparent and effective access to information is crucial if the Tunisian defence sector is to effectively prevent corruption and retain legitimacy, and the government can choose to strengthen its application of law 22-2016. In particular, strengthening the defence sector's accountability mechanisms would limit the risks of corruption that has the potential to contribute to instability within the country. We recommend a clear rationale to the ministry's use of the national security exception, as well as transparency as to how the rationale is applied. To address these threats, Transparency International and I WATCH recommend the following actions:

Develop detailed classification guidelines and a framework for responding to access to information requests within the Ministry of Defence

The Ministry of Defence should develop detailed guidelines to address access to information requests, including how to apply the test which ministry officials may apply when defining the necessary level of classification of a particular document and assessing whether releasing that information could pose a risk to national security The guidelines should be made publicly available, and should be accompanied by training for officials within the ministry responsible for answering access to information requests.

While some types of information can be excluded from access to information requests, no institution or agency should be given a blanket exemption to responding to such requests—even in the name of national security. National security is undeniably important in the defence sector; however, it should be restricted to specific situations. To reduce corruption risks, the MOD should only apply the national security rationale to cases that present a true national security imperative—rather than allowing in to be used as a catch-all phrase to evade accountability towards the public. The Parliament and the INAI should adopt a clear definition of 'national security' and work with the MOD to integrate this into their classification guidelines, to prevent overwhelming use of the national security exception.

Much of the information withheld based on national security, if balanced with the public interest, represents a higher risk of immediate or future prejudice to the public good when withheld. Given ongoing reforms in the defence sector, improving access to information would also empower citizens to understand and monitor progress in the sector and prevent instances of corruption within one of the most opaque and sensitive branches of government.

Proactively publish key information on the Ministry of Defence website

The ministry should develop clear guidelines on which information to publish proactively, and train designated staff to update information on the website on a regular basis, prior to requests being made.

For instance, the website does not currently display the military's annual strategy, budget or audit reports. Regularly uploading and updating this type of information would strengthen the Tunisian public's trust in the accountability of the Ministry to its population. It would also enable citizens to monitor the ministry's progress in implementing its strategy coherently, and guarantee that the public and civil society can play an effective role in identifying corruption risks within the defence sector.

Transparency International Defence & Security

www.ti-defence.org
twitter.com/ti-defence

I WATCH

www.iwatch.tn
twitter.com/IWatchTN