GUIDES TO GOOD GOVERN-ANCE

No. 06

Balancing Openness and Confidentiality in The Defence Sector: Lessons from International Good Practice

Centre for Integrity in the Defence Sector

Norwegian Ministry of Defence

CENTRE FOR INTEGRITY IN THE DEFENCE SECTOR

The Centre for Integrity in the Defence Sector (CIDS) is promoting integrity, anti-corruption measures and good governance in the defence sector. Working with Norwegian and international partners, the centre seeks to build competence, raise awareness and provide practical means to reduce risks of corruption. CIDS was established by the Norwegian Ministry of Defence in 2012.

ABOUT THE AUTHOR

Francisco Cardona is associate international expert at CIDS. Cardona is a renowned expert focused on designing and assessing civil service and public administration reforms, administrative law and justice, anticorruption policies and institution building. His experience stretches from his native Spain, where he developed a career within the civil service, to international organisations, such as the OECD, SIGMA Programme, where he spent 15 years as a senior policy analyst in public governance. At SIGMA he advised a host of some 25 transition and developing countries in Eastern Europe, Africa, Latin America and the Caribbean region. He is trained as a lawyer (Valencia University, 1976) and holds several master degrees in public administration.

FOREWORD

CIDS Guides to Good Governance (GGG) has as their primary objective to present key issues that are of relevance to the field of 'good governance'. The guides should be brief without simplifying matters too much.

In the sixth GGG, the author aims to challenge the concept of confidentiality in the defence sector. In doing so the author asks: « (...) where should the balance between free access to information and restricting that access to some extent» go in a democratic society with an (...) «open government»? Furthermore, when is there a need to restrict information for the sake of national security concerns? See the right of citizens' to State protection.

The guide is written by Francisco Cardona. A CIDS' senior international expert. I would like to thank him for his contribution to such an important topic within good governance. A topic that has been of high actuality in the public debate in recent years and will probably continue to be relevant in years to come.

I would also like to thank the centre's editor, Bård Bredrup Knutsen and our publication coordinator Åse Marie Fossum for their contributions to the guide.

The Centre hopes that this GGG will be utilized by a broad audience, both within the public sector including the defence, as well as outside of the sector. Balancing openness and confidentiality are vital for a well-functioning democratic society.

CIDS is happy to receive any feedback to the guide.

Oslo, 24. April 2018

Per Christensen
Director

CONTENTS

Introduction

This Guide to Good Governance presents a brief view of international good practices from the EU and the OECD countries, aimed at preserving confidentiality of public information in the field of defence and national security while promoting the publics' general right to access information held by public institutions. The aim of this guide is to propose policies that promote open government, access to information and the capacity of citizens to make informed decisions on the performance of governments. At the same time, drawing up boundaries for sound protection of state secrets in those matters that are sensitive to national security, defence, and intelligence matters, as well as the fight against corruption and criminality.

Transparency and publicity are excellent preventive remedies against corruption, maladministration and poor governance. Democracies cannot work properly in secrecy because if secrecy is prevalent, the political regime simply becomes non-democratic since its citizens are excluded from the political process. That implies that the exercise of authority may get out of control and democratic accountability cannot take place. However, public access to information may also have to be restricted in order to preserve the proper functioning of democracy in an efficiently governed state. Therefore, both public information disclosure and certain limitations to that disclosure should equally serve the public interest.

Conceptual framework: National security as a justification for confidentiality

The basic conceptual assumption is that open government and free access to information on the one hand, and restricting that access to some extent on the other hand, benefits the public interest. The internationally accepted general principle is that the 'right to know' shall be promoted by governments, while putting reasonable limits to it in order to protect the confidentiality of certain public information. The latter is necessary if state actions in certain domains, particularly in those concerned with national security and defence, are to be handled effectively.

The main problem with regard to such secrecy is to determine when and how restrictions on public access to information are legitimate. It is an aspirational goal of healthy democracies to ensure proper public access to information while drawing certain legitimate boundaries to limit that access. How to establish an adequate balance between these two considerations is very much dependent on a country's history, societal values and other cultural factors. This is a reason why it is hard to determine whether international standards exist to help reach the right balance (Transparency International UK, 2014). In practice, exact international standards do not exist, although intellectual debates and attempts to establish some overall principles have been numerous in recent years.[1]

If left unchecked, the practice of ensuring secrecy and confidentiality easily becomes sizable and expansive. Certain state services dealing with national security, defence, criminal investigations, intelligence gathering or counter-terrorism have a tendency to apply secrecy to everything they do, even if that result in hindering the citizens' right to know what the government is doing. Apart from the high costs of keeping the "secrecy machinery" working, substantial and expansive use of confidentiality tends to undermine public confidence in governmental institutions and, ultimately, to weaken democratic legitimacy. Too much secrecy also tends to produce more mistakes and wrongdoings than transparency and public scrutiny, as a lack of transparency makes public scrutiny and correction of poor practices more difficult. As a result, in the longer term excessive secrecy may threaten national security more than openness does.

As some public officials have argued – for example, in the United States –too much secre-

1 See The Tshwane Principles (2013): https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

cy "has become an unwarranted obstacle to information-sharing inside and outside of the government, to the detriment of public policy" (Aftergood, 2008, page 400). This points to the problem of over-classification, i.e., that information-holding services tend to classify information to an extent that far exceeds what is actually needed.

The purpose of any classification system is to prevent disclosure of information that could endanger national security, but the vagueness of notions such as "national security" and "security threats" easily opens for excessive use of secrecy. The difficulty of distinguishing between between factual and subjective information makes it hard to establish well-defined criteria for sound classification of information.

Sound classification of information is in itself a very difficult notion, but conceptually we might agree that a "sound" classification is one that is reasonable and departs as little as possible from the democratic values of openness, transparency, and free access to information. In other words, we may agree that a reasonable limitation to transparency is one that a) is exceptional, and b) protects important national security interests. This conclusion acknowledges that there is information in the field of defence and national security whose concealment is *not* critical for the national security and, therefore, may be safely disclosed – totally or partially.

There is still a prevailing traditional approach in some democratic countries where transparency merely represents a citizen's demand, and where secrecy, for the sake of national security, represents the public interest. For example, Mr. Jean Marc Sauvé, deputy president of the French State Council, said in an address to the National Assembly of France, the lower chamber of the French parliament, on 5 July 2011: *"This is the way ahead for drawing the dividing line between the legitimate public interests claiming secrecy and the transparency claimed by the citizens"* (Sauvé, 2011, page 6). This statement builds on the assumption that preserving secrecy protects the public interest, whereas transparency is not in the public interest but only a request driven by the curiosity of citizens and journalists. That is a very dubious assumption. Experience shows that promoting transparency is one of the best ways to protect the public interest, because it contributes to keep public authorities accountable to citizens and other democratic control mechanisms. Transparency, therefore, and not secrecy, may be seen as a means to *bridge* "a gap that arises naturally between the state and its public" (Fenster, 2010, page 619).

There is a broad international consensus that transparency in the policy and actions of public authorities should be the general rule, whereas secrecy should be the exception. Moreover, such exceptions should be justified: they can be defensible only if they are legitimate. They are legitimate only if they can be proven to exist for the sake of protecting genuine national security interests.

The need to distinguish between legitimate versus illegitimate secrecy necessitates some control by authorities that are independent of the classifier.Such independent control mechanisms may be exercised by courts or more specialised public bodies, and their role is to establish whether the national security interests that are invoked to classify information are genuine and sufficiently important. Without external control mechanisms, decisions on

classifying information become exclusively discretionary and, most probably, arbitrary. However, as we will see below, historically courts have played – and still tend to play – a role that is excessively deferential to the withholding of information by security or intelligence agencies.

Conceptually, full transparency is not desirable and probably not possible, as stated above. Furthermore, the state will always operate in certain areas that are obscure or ambiguous. As Fenster (2010, page 623) points out, there is frequently an area in between secrecy and transparency, which means that secrecy is not necessarily the opposite of transparency. In practice, secrecy and transparency do not represent a clear-cut and opposite reality, because both secrecy and transparency require separate institutional bases, and these are structurally different (Riese, 2014, page 14).

More transparency should not necessarily mean less secrecy, but better quality will protect confidentiality. More transparency does mean that only genuine needs for confidentiality will be protected. The institutionalization of transparency policies is relatively new in most countries, whereas the institutionalization of secrecy comes from long established traditions. The values and interests behind each of these traditions are still heterogeneous and somehow inconsistent. The challenge lies in progressively making the institutionalization of the right to know and that of protecting genuine needs for confidentiality more harmonized – in the organizational structures that handle them and in government practices. The search for more consistency between the two policies should ideally be conducive to a single, integrated policy and a more coherent institutionalization of an access to information policy within national governments, in line with national security needs.

However, the notion of "national security" is extremely elusive, as it can mean different things in different national contexts, which complicates the issue further. In the majority of the European countries surveyed by Jacobsen (2013), national security to a varying degree encompasses international relations and domestic security threats as well. In other words, there is not necessarily an obvious borderline.

In order to establish whether or not government secrecy is legitimate, Afterwood (2009, page 402-403) proposes three practical categories of secrecy, while acknowledging that the enduring public policy problem is to separate legitimate secrecy from illegitimate secrecy, and to preserve the former while exposing the latter:

1. **Genuine national security secrecy:**to protect information that would pose an identifiable threat to the security of the nation by compromising its defence or the conduct of its foreign relations. The withholding of such information is not controversial because it is the rationale behind all classification systems, and the public interest is best served when this type of information remains secret.

2. **Bureaucratic secrecy:** the tendency of bureaucrats to protect information, whether out of convenience or on a dim suspicion that disclosure may be riskier than secrecy. This bureaucratic tendency usually leads to over-classification of information and results in an unnecessarily large amount of classified information. It also multiplies the

budgetary costs of secrecy and frequently plays on a bureaucratic feeling of self-importance and an unwillingness to reveal how a specific governmental institution does its job.

3. **Political secrecy:** the tendency to employ a classification for political advantage. This form of secrecy is the most objectionable because it exploits the accepted legitimacy of genuine national security interests in order to advance a self-serving agenda, to evade political controversy or to thwart public accountability. In extreme cases, political secrecy conceals breaches of law, human rights violations, corruption or mismanagement, and threatens the integrity of the political process.

THE GENERALLY WEAK ROLE PLAYED BY THE JUDICIAL IN CONTROL OF CLASSIFICATION SYSTEMS

As indicated above, the courts have traditionally been, and still are, quite deferential in their response to classifying agencies and their so-called *"state secrets executive privilege"*. Judicial deference has helped to cement the idea that national security is too sensitive to be disclosed even to courts (Setty, 2012). A good example from the US is the Cold War hallmark case *United States vs. Reynolds*.[2]

The deferential tendency of the courts towards the executive has been heightened since the September 11 terrorist attacks in the US – frequently referred to as "9/11". Government claims to protect national security have consistently prevailed in court over principles such as accountability, transparency and open government. The many cases in the US, the UK, in France and elsewhere in the democratic world, let alone in less democratic countries, reflect an underlying adherence to a narrow view of the judicial role concerning the review of security-related executive decisions. Unfortunately, this may be to the detriment of the protection of fundamental rights, the rule of law, and respect for genuine security interests.

The "*state secrets executive privilege*" in the USA or the "*public interest immunity certificate*" in the UK, or the "*secret-défense*" in France, are invoked very frequently by classifying executive authorities in order to pre-empt judicial review, or to make it less efficient. Exceptions to openness based on assertions like the three terms above, are regularly accepted by courts even if – sometimes – courts vaguely state that the privilege should be limited to instances of genuine national security only. This quite common judicial stance generally reveals "a judicial disregard of the notion of checks and balances, an abdication of judicial responsibility and a disdain of the structural need to preserve an avenue for plaintiffs to seek redress against government overreaching" (Setty, 2012, page 1573).

Fuchs (2006, page 168), in an outstanding study on the role of courts, found that "given the significant values fostered by the right to access government information, this right should only be sacrificed when a legitimate need for secrecy exists… Neither parliaments nor the public on its own are in a position to challenge excessive secrecy. Independent review constitutes a part of the judiciary's responsibility to ensure that government action is properly authorised". Only courts are independent enough to play the role of challenging excessive secrecy, but seemingly, Fuchs notes, they have refused to accept that role.

2 https://supreme.justia.com/cases/federal/us/345/1/case.html

In nearly all of the European countries surveyed by Jacobsen (2013), the courts have the authority to examine classified information that the government seeks to keep secret on grounds of national security.Notably, however, in some countries, only certain courts or judges with a special clearance may examine classified information.In Germany, only the Federal Administrative Court can examine classified information. In Spain, although the Official Secrets Act does not contemplate access for judges as it does for Congress and the Senate, the Spanish Supreme Court has determined that it, and only it, has the power to review classified information from the Government. The one country in which courts have no authority whatsoever, to directly examine, classified information is France (Sartre and Ferlet, 2010). It seems to be impossible for a French judge to directly examine classified information. In order to limit the effect of this prohibition, a law of 1998 created the French CSDN (*Commission du secret défense nationale*), an independent commission which can access classified information as requested by a judge, in order to evaluate whether it could be reasonable to declassify the information.[3] As goes for the US, the majority of European countries judiciaries normally defer to a public authority's assessment of the fact that disclosure would harm national security concerns (Jacobsen 2013).

CLASSIFICATION CRITERIA AND LEVELS OF CLASSIFICATION

The classification levels have been standardised in such a way that the same system of classification can be found in many OECD countries. Among the OECD countries, a good example of how state secrets are treated is New Zealand. In New Zealand, official information is protected in accordance with criteria based on a strict definition of the necessity to protect official information: Information is to be protected to the extent consistent with the public interest and the preservation of privacy. The classification of such information attempts to grade it on the basis of the damage that would result from unauthorised disclosure, and specifies protective measures to be applied.[4] According to the New Zealand guidelines, in themselves, classifications do not allow official information to be withheld; rather information must be considered on merits using the criteria set up by law.[5] The security classification system of Australia is interesting in the way that it provides clear guidelines for how to classify and de-classify secret information.[6]

The levels of classification in New Zealand, which follows a much-used international practice, are as follows, depending on the public good to be protected:

- National security related: Disclosure would put at risk to the security, defence or international relations of the country, or those of friendly governments, or
- Government policy and/or privacy related: Disclosure would endanger the function of the government or cause loss to a person.

3 http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense

4 New Zealand's Official Information Act of 1982.

5 New Zealand's Guidelines for Protection of Official Information. See https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

6 Australia (2014): Information Security Management Guidelines. Australian Government Classification System. At https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf

Information on national security is protected at the following levels by use of these criteria:

1. **Top Secret**: its disclosure could damage national interests in an exceptionally grave manner:

    - Directly threaten the internal stability of NZ or friendly countries
    - Lead directly to widespread loss of life
    - Cause exceptional damage to the security of NZ forces or allies
    - Cause exceptional damage to the operational effectiveness of NZ forces or friendly forces
    - Cause exceptional damage to the continuing effectiveness of extremely valuable security or intelligence operations
    - Cause exceptional damage to relations with other governments
    - Cause severe long term damage to significant national infrastructure

2. **Secret**: its disclosure could damage national interests in a serious manner:

    - Raise international tension
    - Seriously damage relations with friendly governments
    - Seriously damage the security of NZ forces or friendly forces
    - Seriously damage the operational effectiveness of NZ forces or friendly forces
    - Seriously damage the effectiveness of valuable security or intelligence operations
    - Seriously damage the internal stability of NZ or friendly countries
    - Shut down or substantially disrupt significant national infrastructure

3. **Confidential**: Its disclosure could damage national interests in a significant manner:

    - Materially damage diplomatic relations—cause formal protest or other sanctions
    - Damage the operational effectiveness of NZ forces or friendly forces
    - Damage the security of NZ forces or friendly forces
    - Damage the effectiveness of valuable security or intelligence operations
    - Damage the internal stability of NZ or friendly countries
    - Disrupt significant national infrastructure

4. **Restricted**: Its disclosure could adversely affect national interests:

    - Adversely affect diplomatic relations
    - Hinder operational effectiveness of NZ forces or friendly forces
    - Hinder security of NZ forces or friendly forces
    - Adversely affect internal stability of NZ or friendly countries
    - Adversely affect economic well-being of NZ or friendly countries

Government policy and individuals' privacy are protected at the following levels and by use of these criteria:

1. **Sensitive and Restricted**: Could damage Government interests or endanger citizens:

    - Endanger the safety of any person
    - Seriously damage the economy of NZ
    - Impede Government negotiations
2. **In confidence**: Could prejudice law and order, impede Government business, affect a citizens privacy:

    - Prejudice maintenance of the law
    - Adversely affect privacy of a natural person
    - Prejudice citizen's commercial information
    - Prejudice obligations of confidence
    - Prejudice measures that protect the health or safety of the public
    - Prejudice economic interests of NZ
    - Prejudice measures that prevent or mitigate material loss to the public
    - Breach constitutional conventions
    - Impede the effective conduct of public affairs
    - Breach legal professional privilege
    - Impede Government commercial activities
    - Disclosure or use of information for improper gain or advantage

As already noted, similar markings and criteria for classifying information may be found across many OECD countries. Even in Turkey, where classification rules are not publicly available, certain classification levels are known to exist (Jacobsen 2013). Sweden was the only country which responded to the survey analysed by Jacobsen (2013) in which the law does not specify levels of classification of information, because in Sweden classification serves a purely administrative function.

Other aspects related to classification of information (e.g. classification procedures, marking requirements, classification authority, duty to give reasons for classifying, accountability for improper classification, oversight bodies, etc.), vary quite significantly across European countries (see Jacobsen 2013 and Transparency International UK, 2014).

DE-CLASSIFICATION CRITERIA

In European countries, the de-classification of information is shaped by three main criteria: time limits, trigger event, or mandatory review period. The main purpose is to prevent perpetual classification of information. However, it is not rare to find countries where no criteria for de-classification are provided in legislation or in administrative practices. The median time limit for classification, according to the calculation made by Jacobsen (2013), is 30 years among European countries, with specific time limits ranging from 10 years in the Netherlands to 100 years in Romania to indefinite in Spain and Turkey. The latter, however, is quite exceptional in Europe.

The most common period for mandatory review of classified information is 5 years. In Sweden, there is no pre-established mandatory review, but the classification of any kind of information must be reviewed whenever a request for information disclosure is made. Automatic de-classification (trigger event) varies across countries, but in the majority of them, the main aspect is a governmental discretionary decision to de-classify various classes of information. Such a decision can also be the consequence of an Access to Information Act procedure undertaken by a citizen or civil organisation.

TESTING TO KEEP SECRECY UNDER CONTROL: THE HARM TEST AND THE PUBLIC INTEREST BALANCING TEST

According to *Right2INFO.org*, a NGO promoting good law and practice, the so-called Harm Test and Public Interest Test originate from the requirement that restrictions on the right of access to information have to be proportionate and necessary.[7] OECD-SIGMA (2010) provides an extensive and thorough conceptual approach to the notions behind these tests, flowing from a distinction between absolute restrictions versus relative restrictions concerning access to information. Among the former, those having to do with defence and national security are generally included.

THE HARM TEST

In accordance with the Harm Test, a public authority must demonstrate that disclosure of certain information threatens to cause harm to a protected interest. Therefore, disclosure should not take place. The Harm Test requires that the state validates a risk of a substantial and demonstrable harm to a given legitimate interest. It must be demonstrated that the limitation is related to an identified legitimate interest, and that disclosure would cause substantial harm to that interest. Such harm should be sufficiently specific, concrete, imminent and direct, and not speculative or remote.

THE PUBLIC INTEREST BALANCING TEST

The Public Interest Balancing Test refers to proportionality. This requires a balancing act, whereby the harm of disclosure is assessed against the public interest that might be served through disclosure. The conditions under which an explicit and detailed public interest may outweigh the claim for secrecy/confidentiality, need to be specified through national legislation. According to many national classification models – including the Inter-American and the African – the public interest becomes mandatory and overrides other interests in the case of information related to human rights violations or crimes against humanity. The Balancing Test requires that a public authority, or oversight body, weighs the harm that disclosure would cause to a certain protected interest against the public interest served by disclosure of that information.

The definition of what constitutes a public interest varies across countries and often requires a case-by-case assessment. In general, public interests favouring disclosure usually involves matters of public debate, public participation in the political debate, accountability for the allocation and the spending of public funds, and issues of public safety. Issues related to public safety and the environment, significant threats to health, and information related to grave human rights violations, are generally considered to justify mandatory priority of the publics' interest to disclose information.

Some countries have issued guidelines for the administrative procedures of civil servants. For example, in New South Wales, Australia, when deciding whether to release information, public employees must apply the Public Interest Balancing Test. This means that they must weigh the factors in favour of disclosure against the public interest factors against disclosure.[8] According to these guidelines, the Public Interest Balancing Test involves three steps:

1. Identify the publics interest in facour of disclosure.

7 http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

8 http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

2. Identify the publics interest against disclosure.

3. Determine the relative weight of the publics interest in favour of and against disclosure and determine where the balance between those interests lies.

Despite the clear stance of the Australian legislation in favour of the disclosure of information, the provincial laws on access to information establish a number of situations where the presumption is in favour of withholding the information and protecting secrecy. The most prominent is the information that is subject to an overriding secrecy law, 26 Acts are specifically named. This follows a general tendency affecting many OECD countries, whereby the Freedom of Information Acts (FOIAs) in practice have ceased to be relevant at the doorstep of traditional legislation conserning state secrets. States secrets are consistently kept out of the scope of freedom of access to information legislation. In addition, there has generally been made little efforts in most countries to harmonise the traditional state security legislation with new legislation conserning freedom of access to public information.

The fact that many FOIAs have left national security-related secrecy virtually untouched means that legislation and recourse to courts so far have proved less effective as instruments for reducing the universal trend towards increased use of confidentiality and secrecy in the works of security and intelligence agencies. Such institutions, with their traditional and frequently opaque way of dealing with confidential information, basically remains unaffected by FOIAs, despite a broad international trend in favour of more public transparency and civil society demands for the "right to know".

This points to the fact that enacting general legislation which is effective in balancing secrecy and openness is challenging, both conceptually and in practice. One reason is that public bodies or agencies that are the most likely to classify information, tend to have quite different purposes and motivations in their work and practices. That fosters different security-related administrative cultures. For example, military bodies tend to focus primarily on the security of weapons technology and operational plans, intelligence agencies on the protection of sources and operating methods, diplomats are concerned with the international consequences of the classification and the de-classification of diplomatic information, and the police are eager to protect their informants and operational plans. This leads each agency or institution to develop its own guidelines, procedures, and protocols – which tend to remain in force for years, unscrutinised and without serious review. Furthermore, it is understandable that within agencies such as those listed above, people tend to play on the safe side in order to avoid unwarranted problems, which often leads to the symptom of over-classification (Aftergood, 2009).

As a result, informed observers and practitioners suggest that, even if the classification should be done by the relevant agency, the de-classification authority should lie outside of that agency. This is the best way to nullify an agency's self-interest and purge it from classification excesses (Aftergood, 2009, page 412). Some successful attempts to do so have been carried out in the United States as, for example, through the *Interagency Security Classification Appeal Panel* (ISCAP)[9] and the *Fundamental Classification Policy Reviews* (FCPR).[10] In France,

9 https://www.archives.gov/declassification/iscap

10 https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf :See also the 1994

the CSDN represent another example (see above). The American experience, described by Aftergood (2009), in essence shows that "if one agency cannot successfully explain to and convince a senior official or panel from other agencies why the national security requires that a certain item is classified, then there is reason to doubt the necessity of its continued secrecy".

CONCLUSIONS

1. Legislation regulating confidentiality of information in the fields of security and defence is needed and should be as precise as possible. Such legislation should provide criteria for classifying and de-classifying information, while taking into account that the legislation by definition is going to be general and consequently the specified criteria will also be general. Legislation regulating confidentiality, which in many countries precedes legislation on free access to information, should be harmonised with the latter, in order to prevent inconsistencies in the national legal order.

2. Along with a sound legal framework, a conscious and skilful management at the agency level is necessary to apply the classification legal criteria in a judicious or sensible way, in order to foster democratic values and the principle of public transparency to the largest extent possible. A conscious understanding of the need to balance different considerations should be part of the organisational culture. The managers of the agencies in question should see it as their role to attain a balanced approach between legitimate confidentiality and legitimate transparency.

3. To reduce unjustified over-classification and to balance the public's right to know and national security imperatives – and other legitimate reasons for secrecy – are challenging endeavours. To transform a culture of secrecy to one of transparency in the area of defence is probably out of reach within the foreseeable future in most EU and OECD countries.[11]

4. Loyalty, respect for established procedures, and discreetness are expected from employees and others working in the field of security and defence. These qualities are indeed required but, nevertheless, a certain degree of innovation and new ideas could and should be encouraged, even if the room for changes may prove modest. Nevertheless, there is a need to take a critical view on how to achieve an optimal balance between legitimate secrecy on the one hand, and legitimate access to information on the other.

5. The personnel in charge of implementing secrecy laws or confidentiality policies should be especially trained to be able to accord the necessary weight to the democratic need for openness and transparency in government while also discerning clearly, in the light of legislation, what needs to remain hidden from the public eye. The alternative to indiscriminate secrecy is not indiscriminate openness. The quality and competence of the staff working in the field of security and defence are of the utmost importance since that has direct implications for a democratic society and the relations between security agencies and civil society.

pioneering review in the Energy Department at: https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html

11 Even if Romania seems to have managed to do so (Matei, 2007).

6. An independent institution, for example an interagency de-classification commission – located beyond the exclusive remit of the most important classifying agencies, i.e. the military, intelligence and police – should have the competence to review and periodically de-classify information held secret by individual agencies. In general, courts have proved to be too deferential to state secret executive privilege, and there is limited reason to expect a change in that regard.

7. A good practice seems to be emerging that implies reduced discretionary practices compared to what has characterised traditional classification practices: Classification and de-classification of information should be decided upon not by an individual, but by an independent committee or commission, able to carry out impartial judgements on the necessity either to classify or de-classify a given piece of information – totally or partially. Such a specialised unit should be guided by legally established criteria in order to determine harm and perform balancing tests. Membership of such an independent committee or commission should be limited, for example 5 to 7 members, and could encompass security expertise under the executive, the parliament, the MPs and the ombudsman, and the judiciary.

REFERENCES

Aftergood, Steven (2009):"*Reducing Government Secrecy: Finding What Works*," in Yale Law & Policy Review

Vol. 27, No. 2 (Spring, 2009), pp. 399-416. Available at: https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010): *Seeing the State: Transparency as Metaphor*, in Administrative Law Review, pages 617-672, available at http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006): *Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy*, in Administrative Law Review, Volume 58, Number 1, Winter 2006, pages 131-176.

Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. Available at: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007): *Reconciling Intelligence Effectiveness and Transparency: The Case of Romania*, in Strategic Insights, Volume VI, Issue 3 (May 2007). Available at: https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OECD (2010), "*The Right to Open Public Administrations in Europe: Emerging Legal Standards*", SIGMA Papers, No. 46, OECD Publishing, Paris. At: http://dx.doi.org/10.1787/5km4g-0zfqt27-en

Riese, Dorothée (2014): *Secrecy and Transparency*, paper resented at the ECPR Conference in Glasgow , September 3-6, 2014. Available at: https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

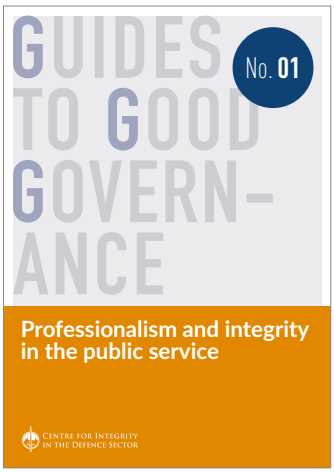
Sartre, Patrice & Ferlet, Philippe (2010): *Le secret de défense en France* in Revue Études 2010/2, Tome 412, février, pages 165-175. At : https://www.cairn.info/revue-etudes-2010-2-page-165.htm

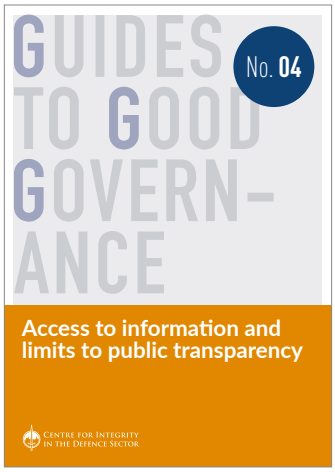
Sauvé, Jean-Marc (2011): *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général*, discours à l'Assemblée Nationale le mardi 5 juillet 2011 au colloque organisé par Transparence Internationale France. Disponible à : http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

Setty, Sudha (2012): *The Rise of National Security Secrets*, in Connecticut Law Review, volume 44, number 5, July 2012, pages 1563-1582.

Transparency International UK (2014): Classified Information: A Review of 15 Countries. Available at: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

Guides to Good Governance series




GUIDES TO GOOD GOVERN-ANCE
No. 04
Access to information and limits to public transparency
Centre for Integrity in the Defence Sector


GUIDES TO GOOD GOVERN-ANCE
No. 05
Managing real estate corruption and fraud risks in the defence sector
Centre for Integrity in the Defence Sector

Guides to Good Governance is a series of small booklets each of which discusses a particular topic of importance to good governance in the defence sector. The guides can be read by individuals with an interest in learning more about one or several topics of direct relevance to good governance in the defence sector – or the public sector more generally – and they can be used for educational purposes.

Published by: Centre for Integrity in the Defence Sector
Design: www.melkeveien.no
Print: Norwegian Government Security and Service Organisation
May/2018. Impressions: 100

CENTRE FOR INTEGRITY
IN THE DEFENCE SECTOR

www.cids.no