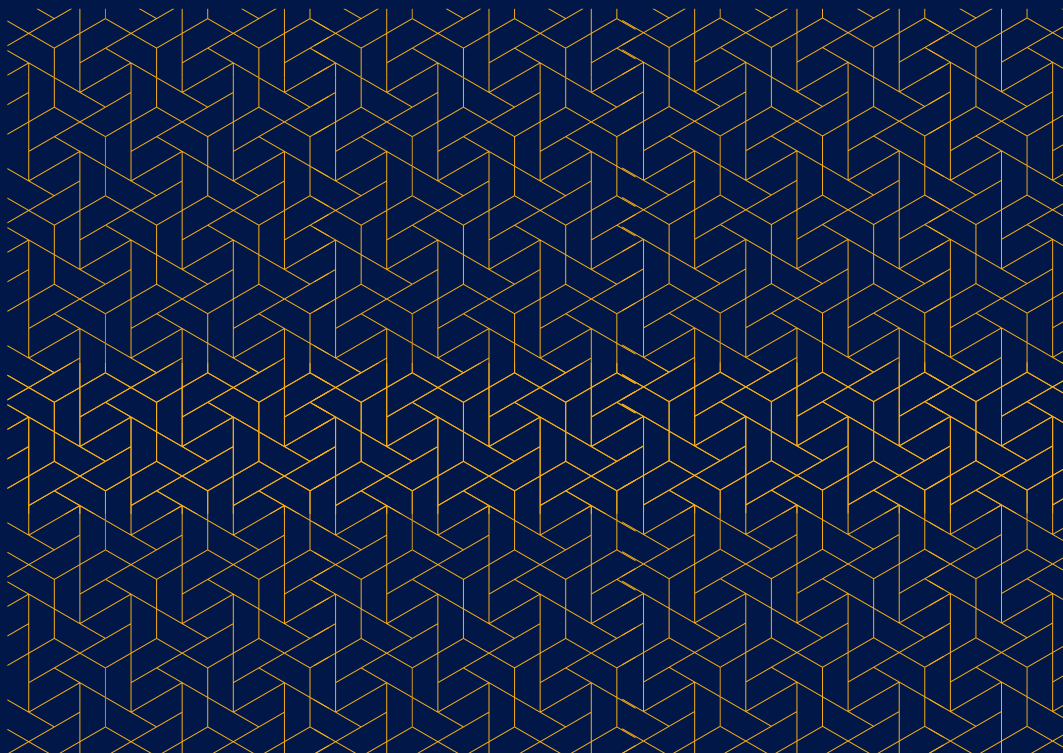
DCAF Geneva Centre for Security Sector Governance

THEMATIC BRIEF

Vetting of the Members of Parliament



About this thematic brief

The thematic brief was prepared by SIPOL Team at Europe and Central Asia Division. DCAF would like to thank the Federal Department of Defence, Civil Protection and Sport (DDPS) of the Swiss Confederation and the Norwegian Ministry of Foreign Affairs for its generous support in making this publication possible.

Note

The opinions expressed in this publication are those of the authors and do not reflect the opinions or views of the Federal Department of Defence, Civil Protection and Sport of the Swiss Confederation and the Norwegian Ministry of Foreign Affairs.

About DCAF

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

DCAF - Geneva Centre for Security Sector Governance
Maison de la Paix Chemin Eugène-Rigot 2E CH-1202
Geneva, Switzerland

Tel: +41 22 730 94 00

info@dcaf.ch www.dcaf.ch

Twitter @DCAF_Geneva

ISBN: 978-92-9222-578-0

VETTING OF THE MEMBERS OF PARLIAMENT

Introduction

In liberal democracies, parliaments exercise oversight over the security sector, including intelligence services.[1] This is usually conducted by a standing select committee with cross-party representation. Such committees normally take one of two forms: specialized committees dealing exclusively with oversight of intelligence, or committees with broader mandates, responsible for oversight of the whole security sector.

Given that intelligence services operate in clandestine fashion, great care must be taken to address concerns regarding the protection of their assets, methods, operations, and other classified information. Accordingly, the effectiveness of the parliamentary oversight committees is dependent on their ability to access relevant classified information. Individuals whose work requires access to classified information may be required to undergo a process of vetting. Concerns remain as to whether such vetting procedures are equally applicable to members of parliaments, and if so, which body should be responsible conducting them. This is particularly the case for countries in which intelligence services are themselves responsible for the vetting process, with some arguing that this may challenge effective parliamentary oversight. To this end, this Thematic Brief outlines two approaches to the vetting of members of parliament (hereinafter referred as MPs). For each, the general standards and procedures are detailed with reference to case studies; with the limitations of each approach, as well as possible strategies to overcome these, also presented. The Brief concludes by identifying recommendations based on best practice and internationally recognized norms, which underscores that regardless of the approach taken, suitable mitigating policies should be enacted.

1 These include, for example: Belgium – Standing Intelligence Agencies Review Committee; Netherlands – Review Committee on the Intelligence and Security Services; Portugal – Council for the Oversight of the Intelligence System of the Portuguese Republic; and Sweden – The Commission on Security and Integrity Protection.

The Two Approaches

The existence of -and procedure for the vetting of members of parliamentary oversight committees (MPs) is highly contested, even among liberal democracies. While approaches vary, two general models are in use in Euro-Atlantic countries - the Legalistic Approach and the Informal Approach. Despite the differences in each, they are united in that parliament remains the final arbitrator: through adopting related legislation, it decides on whether or not MPs on intelligence oversight committees should be subject to vetting.

Approach 1: Legalistic - the requirement of formal security vetting for MPs for membership of parliamentary committees responsible for the oversight of intelligence services

Description: Formal security vetting is used in several countries in the Euro-Atlantic area. This approach reduces the risks associated with access to classified information as formal security vetting is generally applied to most if not all staff and appointed officials (mostly in the executive branch) that require access to classified information, including MPs. According to a 2018 analysis conducted by NATO Parliamentary Assembly and DCAF on Parliamentary Access to Classified information, the countries which require vetting of MPs in order to access classified information include Albania, Canada, Hungary, Latvia, Lithuania, Belgium, North Macedonia and Romania.

A distinction should be drawn between the entity conducting security background checks and the entity issuing the security clearance. These two competences can either be delegated to a single authority (i.e. in the case of Romania, the National Register for State Secret Information), or divided between two entities to ensure the separation of powers. In the case of the latter, background checks can be done by domestic intelligence agencies, an independent governmental entity or an external institution. For example, in the United Kingdom vetting is conducted by United Kingdom Security Vetting (UKSV), a department of the Cabinet office separate from its domestic intelligence agency, known as The Security Service (MI5).[2]

Under this approach, security clearances are commonly issued either by the parliament or a government agency – most often the national security authority, domestic intelligence service or police. In Canada, for example, vetting is conducted by the Royal Canadian Mounted Police and the Canadian Security Intelligence Service, while security clearances are issued by the Privy Council. In Albania, security clearances are issued by the Directorate of Security of Classified

2 UKSV transitioned in April 2020 from being part of the Ministry of Defence, into the Cabinet Office

Information in consultation with the State Intelligence Service. In Latvia, the Constitution Protection Bureau conducts vetting, and the decision to issue security clearances is made by the National Security Authority, which is the sub-division of the Bureau. Similarly, in Hungary the Constitution Protection Office conducts vetting, but the decision to issue security clearances rests with the director of the Constitution Protection Office, or the Ministry of Interior.

Background checks are conducted to provide a risk assessment as regards individual affiliations, interests or vulnerabilities that could lead to the disclosure of classified information for financial or political gain, or through 'blackmail'. If undertaken correctly, formal vetting processes act to build between confidence between oversight bodies and intelligence agencies through ensuring that members of the former do not disclosure classified information. This is particularly important in states going through a process of democratic transition, where security agencies are generally reluctant to share classified information.

While in certain countries vetting is not generally required in order for MPs to access classified information, it can be a condition to access certain types of classified information, such as those provided by foreign intelligence agencies (e.g. Norway, Estonia and Croatia) or information classified as 'top-secret' (e.g. Poland). In Norway, such vetting is conducted by the Storting (Parliament). In Estonia, Croatia and Poland, it is done by the intelligence services. In the case of Estonia, it is the responsibility Internal Security Service or the Foreign Intelligence Service, while the discussion to issue related security clearances is made by the Security Authorities Oversight Committee of the parliament. In Croatia, the National Intelligence Agency conducts vetting, with security clearances issued by the Office of the National Security Council; and in Poland, vetting is done by the Internal Security Agency, and the decision to issue security clearances by its director.

Limitations:

- Conflicts with the principle that MPs be able to access information of any type: The requirement that MPs wishing to access classified information - whether in pursuit of membership to oversight committees or due to the type of information sought - undergo formal vetting conflicts with the generally held principle that by virtue of being elected, MPs should have the right to access information without constraint.
- Provides the opportunity for intelligence service to influence appointment processes: Concerns may also arise when states use models in which intelligence services are involved in vetting procedures. Such a model in theory provides intelligence services with the ability to intervene in the selection process

of members to oversight committees. For example, in countries where intelligence services are involved in issuing security clearances, potential members of oversight committees may be refused such clearances if the intelligence services in question deems it favorable to their interests. Conversely, in countries in which intelligence services are involved in background checks, they may seek to discredit prospective members of oversights committees in order that the authority responsible for issuing the security clearance refuses to do so.

- Lack of inclusion of minority political parties in oversight committees: In one-party dominated parliaments in which the decision to issue security clearances rests with the parliament, such an approach could lead to the marginalization of minority parties. This could challenge the effectiveness of oversight committees, as their political affiliations might result in a reluctance to challenge the decisions of the executive.

Mitigating Policies:

- Separating functions and responsibilities in the vetting process: Under this approach, vetting would be conducted by an external institution, which would either issue the security clearance or submit its recommendations to an independent body or parliament, who would then issue the clearance. For example, in the United Kingdom vetting is conducted by the United Kingdom Security Vetting (UKSV), which is part of the Cabinet office, and therefore fully independent from the intelligence services. Such an approach may reduce potential bias or manipulation of the vetting process in that intelligence agencies would still conduct background checks, but the decision to issue security clearances would rest exclusively with another institution, most often the Parliament. In this case, informal compromises between the political parties represented in parliament could be achieved, while the possibility for MPs with dubious records to be 'quietly' disqualified from being considered as committee candidates would exist.
- Establishing mechanisms through which decisions made by an intelligence agency on issuing security clearances be consultative or advisory: In countries where intelligence services issue or are involved in issuing of security clearances, this approach would instead render their decisions purely consultative or advisory. As such, the final decision to issue a security clearance would rest with the parliament or government. This could take place through a parliamentary procedure. Even if such a procedure does not typically challenge the recommendations or an intelligence agency, the separations of roles carries with it symbolic significance

- Providing for an appeals procedure: Under this approach, the law should provide for an appeals procedure for cases in which a security clearance is denied. Such a procedure should include the obligation to justify on the part of the intelligence agency why a security clearance was denied. Such an approach is used in Romania, where MPs have the right under law to know why their security clearance was denied.

Approach 2: Informal - no requirement of formal security vetting for MPs for membership of parliamentary committees responsible for the oversight of intelligence services.

Description: This approach is the most widely used in Euro-Atlantic countries, including Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Germany, Greece, Iceland, Italy, Luxembourg, Montenegro, Norway, Netherlands, Poland, Portugal, Slovakia, Slovenia and Spain. It is grounded in the principle that by virtue of being elected as public representatives, MPs should have the right to access information without constraint. Such an approach assumes that the vetting of MPs would be a violation of the separation of powers as it may restrict membership to oversight committees. In cases where a government body or executive issue security clearances, it may also lead MPs to become overly acquiescent to the executive to increase the chances of being issued with security clearances, thereby conceivably undermining their important role of holding the executive to account. Under this approach, it remains possible to prosecute MPs to prevent or punish the unlawful disclosure of classified information. MPs are also required to take an oath of secrecy after being elected to an oversight committee. In some cases (e.g. Croatia), such MPs are also required to sign specific documents acknowledging their liability in cases in which they unlawfully reveal classified information.

In EU and NATO countries using this approach, MPs are nevertheless required to undergo a formal vetting procedure if they wish to have access to classified information from another EU or NATO member state. Depending on the mandate of the oversight committee, MPs may therefore still require security clearances, and therefore be subject to vetting.

Limitations:

- Reduces trust on the part of intelligence services: This approach has been criticized on the grounds that it may create mistrust between oversight bodies and the intelligence community. The argument contends that in the absence of formal vetting procedures for MPs, intelligence agencies may feel that classified information may be more easily disclosed. In practical terms, this may manifest in decreased cooperation between the two and, in particular, a reluctance of intelligence services

to voluntarily disclose certain information, possibly reducing the ability of oversight committees to perform their oversight functions effectively.

- Increases the risk of the disclosure of classified information: In theory, in the absence of a formal vetting procedures, the affiliations, interests or vulnerabilities of certain MPs may increase the chances of them disclosing classified information to foreign adversaries -whether deliberately or otherwise - potentially jeopardizing the assets, methods or operations of intelligence services, or state secrets.

Mitigating Policies:

- Clear rules on access to classified information: Clear rules and conditions shall be established to receive classified information that ensure fundamental principles and standards of security are safeguarded. These rules should be derived from the mandate of the committee to ensure that it can effectively conduct its function. The legislation should provide clear guidance on the circumstances under which MPs can share or discuss the information with third parties or other members or the service and whether the permission of the intelligence agency is necessary under any circumstances.
- Clear regulations governing unauthorized disclosure: Criminal penalties, civil and administrative measures shall be outlined in national legislature in order to deter unauthorized disclosures. The role of intelligence agencies and/or national security agency in handling unauthorized disclosure of information shall also be clearly defined.

RECOMENDATIONS

This Thematic Brief has demonstrated that approaches to the vetting of members of parliamentary oversight committees vary considerably across the euro-Atlantic sphere. While both approaches are applied, they are both grounded in the principle of parliamentary supremacy – namely that through adopting related legislation it is parliament who decides on whether or not MPs on intelligence oversight committees should be subject to vetting. Despite this, both approaches bring with them advantages and limitations. While the Legalistic Approach benefits from reducing the chances of classified information being unlawfully or unintentionally disclosed, and thus facilitates trust between intelligence services and oversight committees, it suffers from providing intelligence services with the opportunity to influence appointment process. In addition to implementing the mitigating strategies outlined above, if this approach is chosen, the process of vetting must be transparent, legally defined and conducted in a fair manner, preferably by an independent body. Further, background checks should be time-bound, and the findings considered state secrets and are treated as such.

While the Informal Approach overcomes some of limitations with the Legalistic approach through not subjecting MPs to formal vetting, it may increase the risks of classified information being disclosed and create mistrust on the part of intelligence services, potentially thwarting cooperation and voluntarily information sharing with oversight committees.

In addition to the mitigating strategies outlined for each approach, several general considerations should be taken into account when design approaches towards vetting. These are outlined below, and are no less applicable to approaches in which members of parliamentary oversight committees are not subject to formal vetting:

- Representation of other political parties: Internal parliamentary rules should provide for the representation of members of other political parties in oversight committees to prevent government control of intelligence agencies. Such rules are common-place Euro-Atlantic countries, such as in the Tweede Kamer's Intelligence and Security Services Committee of the Dutch Parliament, which is composed of the leaders of all parties in parliament. An alternative approach is for a member of an opposition party to chair parliamentary oversight committees, an approach used in Italy, Hungary, Slovakia and Slovenia.
- Clearly defining access to classified information in mandates, laws, and procedures: The ability of MPs to access classified information should be clearly defined in the mandate of the

oversight committee and based on the "need to know" principle. It must also be clearly defined in law or parliamentary rules of procedure. Failing this, the responsibility to define how and under what conditions MPs may access classified information falls to the executive and to ministerial discretion, with the oversight committee having no recourse to challenge such decisions.

- Restricting access to certain types of classified information: Oversight committees should be restricted from accessing information related to ongoing intelligence operations. Without such restrictions, members of oversight committees may be able to influence such operations. In addition, information concerning the assets of -and methods used by intelligence services should be not be available to oversight committees in cases where such information originates from foreign entities or relates to judicial proceedings or ongoing criminal investigations.
- Training for members of oversight committees on handling classified information: Training should be provided to members of oversight committees on the handling of classified information, with a particular focus on appropriate methods and techniques through which such information may be shared. Such trainings should include both conceptual and physical aspects of protection of classified information and will help ensure that such information is not accidently leaked.
- Restricting the movement of classified information: MPs should not be permitted to remove classified information from the premises of security and intelligence services. In addition, the provision of classified information should be conditioned on MPs having the appropriate facilities for their storage, and all such information should be officially logged.
- Accessing providers of classified information: MPs should have the ability to question intelligence officials responsible for the procurement of classified information on issues concerning their assets, methods and operations (excluding ongoing operations, judicial proceedings or criminal investigations, or information procured from foreign intelligence services).
- Accessing technical expertise: Many countries within the Euro-Atlantic sphere, including Denmark, the Netherlands, and the UK, have established independent/expert oversight committees, generally composed of retired security sector officials or experts with a legal background. Members of parliamentary oversight committees should have access to the technical expertise of such expert committees, who generally

work full-time and thus are able to provide more in-depth and comprehensive information.

- Applying the 'Need to Know' Principle: Regardless of whether MPs are subject to formal vetting or not, information should be restricted based on the 'Need to Know' principle. In practice, this means that MPs would only be provided classified information it is necessary to perform their oversight mandate; the purpose being to discourage the 'free browsing' of sensitive materials and their misuse for personal interest. Nevertheless, when interpreted strictly it could also limit the access of committee members to information necessary to fulfil their function. For this purpose, limits on access to information should be clearly defined in law, or related parliamentary rules and procedures. Without such safeguards, the responsibility to define access to classified information by MPs in relation to the 'Need to Know' principle would rest exclusively with the executive or via ministerial discretion, providing oversight committee members with no redress.
- Providing clear regulations for the sharing of classified information: Clear obligations should be established to prevent the discussion of sensitive or classified material by MPs with anyone who does not have the right to receive such material.
- Ensuring a clear and comprehensive legal framework: The above-mentioned measures should be clearly defined in a state's legal framework, including laws, sub-laws, and internal regulations, with clear written guidance on their implementation. Such a legal framework should also extend to the punishments incurred for the unlawful disclosure of classified information.

ANNEX

Case study: United Kingdom

All members of the Intelligence and Security oversight committee and their staff are vetted to the highest 'Developed vetting' level. This includes: 1) the obligation to complete a general security questionnaire which covers information such as personal details, family members, professional and personal connections, friends, foreign travel, medical history, social media profile and history, internet usage, membership of organizations, education and work history; 2) the obligation to complete a financial questionnaire which covers financial aspects of the individual and their close family members, including bank accounts, investments and income; 3 and) interviews conducted by nominated security vetting officer (A – an individual interview which includes intrusive questioning covering such things as their views on various matters, lifestyle and what they have said on the forms; B – Interviews of five referees nominated by the individual; and C – Interviews of previous employers). This process normally takes at least two months. The security clearance is normally renewed every five years and each applicant is asked to fill in an annual questionnaire to cover any changes in personal circumstances. A decision to withdraw an MPs security clearance can only be done by the Prime Minister based on a recommendation of a security vetting officer.

The access to secret material (i.e. files, operations or methodologies) is specifically covered in the legislation on Security and Intelligence Services. The ISC may examine expenditure of the service at a macro level (i.e. not operational level), administration of the service (including general management and human resources policies, salary and pension policies) and policy of the service (what the service is required to do by government and how does it go about its tasks). The ISC can also oversee operations of the service, but only when it is of national interest, in that it affects the nation as a whole. They are not allowed to review any ongoing or live operation, except following a special request of the Prime Minister to investigate the matter or a special request by the head of the service.

DCAF Geneva Centre for Security Sector Governance

www.dcaf.ch

DCAF – Geneva Centre for Security Sector Governance
Chemin Eugène-Rigot 2E
P.O. Box 1360
CH-1211 Genève 1