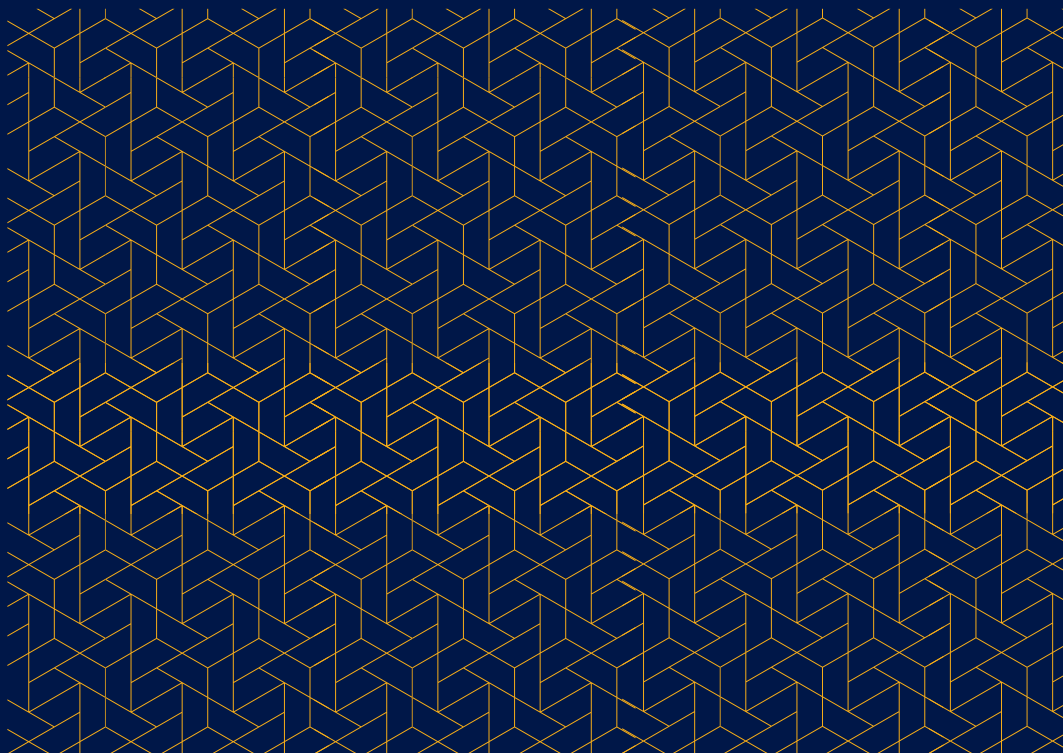
DCAF Geneva Centre for Security Sector Governance

THEMATIC BRIEF

INTERNAL CONTROL IN INTELLIGENCE SERVICES



About this Thematic Brief

This Thematic Brief was prepared by DCAF's 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 their generous support in making this publication possible.

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

Cite as: DCAF – Geneva Centre for Security Sector Governance. 2022. Internal Control in Intelligence Services. Thematic Brief (Geneva: DCAF).

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 or the Norwegian Ministry of Foreign Affairs.

Copy-editor: Alessandra Allen

Design & layout: DTP Studio

ISBN: 978-92-9222-635-0

Table of Contents

List of Abbreviations and Acronyms 4

Introduction 5

Definitions and terminology 6

1. Establishing a Comprehensive Legislative Basis for Effective Internal Control 7

2. Key Components of an Internal Control System 10

3. Challenges to Internal Control 15

Recommendations 19

List of Abbreviations and Acronyms

BND German Federal Intelligence Service (Bundesnachrichtendienst)

KSK German Special Forces Command (Kommando Spezialkräfte)

MENA Middle East and North Africa

NSA US National Security Agency

SOP Standard operating procedure

Introduction

Intelligence services are specialized state agencies responsible for producing intelligence relevant to the security of the state and its people.[1] Intelligence services should act within a framework of democratic control, the rule of law, and respect for human rights. To achieve this, states have developed extensive oversight and control systems. While these systems vary, they are generally executed by a range of institutions and actors within a state, and typically include five components: **external oversight**[2] by the executive, legislative, and judicial bodies; **independent oversight** by ombuds institutions and supreme audit institutions; **public oversight** by civil society organizations and the media; **internal control**[3] by the senior management of intelligence services; and **executive control** by the appropriate executive authority.

Considerations of oversight and control of intelligence services usually focus on external oversight through parliamentary committees, the judiciary, or the executive. Less emphasis is placed on internal control mechanisms within the services. The importance of internal control should not, however, be underestimated. First, a lack of effective internal control prevents external oversight bodies, such as parliamentary committees, from fulfilling their role effectively. Intelligence service managers play a crucial role in facilitating scrutiny by oversight bodies not only by ensuring that major infractions are reported to the appropriate authority, but also by creating an environment that encourages cooperation with oversight bodies.[4] Second, while transparency is essential to maintaining democratic control of government, intelligence services require a significant degree of secrecy to be effective. Consequently, intelligence services are subject to highly restricted oversight, unlike other public institutions. Effective internal control is therefore essential to rectify this inherent (and unavoidable) imbalance by ensuring that the day-to-day work of intelligence services is carried out in accordance with the law and

1 For more information, see: DCAF – Geneva Centre for Security Sector Governance. 2017. 'Intelligence Services', SSR Backgrounder Series (Geneva: DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf

2 For more information, see: DCAF. 2015. 'The Security Sector', SSR Backgrounder Series (Geneva: DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_3_The%20Security%20Sector.11.15.pdf.

3 For more information, see: DCAF. 2017. 'Intelligence Services', SSR Backgrounder Series (Geneva: DCAF). Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf.

4 Born, Hans and Aidan Wills (eds.). 2012. Overseeing Intelligence Services: A Toolkit (Geneva: DCAF), p. 9. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/Born_Wills_Intelligence_oversight_TK_EN_0.pdf.

with respect for human rights. Third, to avoid undue influence and ensure independent, objective analysis, intelligence services must retain a degree of autonomy from the executive. Executive control over intelligence services is therefore sometimes less pronounced,[5] meaning that effective internal control is vital to ensuring intelligence services act within the rule of law.

For the above reasons, intelligence services should be subject to both effective oversight and internal control. This Thematic Brief addresses the latter by examining internal control systems used in Euro-Atlantic countries. The Brief is divided into five sections. The first section defines key terms and concepts, and clarifies the scope of the Brief. The second details the key prerequisites for an internal control system, focusing on the role of the executive branch in establishing legal parameters for intelligence services. The third examines the key characteristics of internal control systems. The fourth outlines common challenges to ensuring effective internal control, and the final section provides recommendations on how to overcome these challenges.

Definitions and terminology

The concepts of **control and oversight**, while similar, are not the same: 'Control implies the power to direct an organization's policies and activities, for example by making rules, codes or policies that determine how an organization functions. Oversight means verifying whether rules and laws are obeyed, and codes and policies are applied.'[6]

While no formal definition of **internal control** exists, for the purposes of this Brief it is understood as the 'rules and processes within an intelligence service to ensure staff perform professionally and effectively within the limits of their authority, in compliance with the law and with respect for human rights, including gender equality'.[7] This understanding of internal control emphasizes the role of internal rules and processes in preventing, investigating, and reporting wrongdoing and abuse of authority.

Although the terms **internal control** and **executive control** are often used interchangeably, they are not synonymous. While they both imply the ability to direct an organization's policies or activities, the level of

5 This in part depends on whether executive control is indirect or direct. For more information, see: DCAF. 2017. 'Intelligence Oversight', SSR Backgrounder Series (Geneva: DCAF), p. 6. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_11_Intelligence%20Oversight.pdf.

6 DCAF. 2017. 'Intelligence Oversight', SSR Backgrounder Series (Geneva: DCAF), p. 3. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_11_Intelligence%20Oversight.pdf.

7 Ibid, p 6.

authority of the body who exercises such powers differs: in general, internal control is executed by senior intelligence service managers (that is, directors, assistant directors, or heads of departments or of separate units within the service), while executive control is executed by the government ministry to which the intelligence service is subordinated – or in cases where a service falls under the direct control of the executive, by the president or prime minister's office or a joint executive body such as a national security advisory board.[8]

External oversight is understood as the process through which the executive, legislative, and judiciary verify whether services comply with laws and rules and properly apply codes and policies. **Independent oversight** and **public oversight** seek to fulfil the same function, but they are the responsibility of different actors – namely ombuds institutions and supreme audit offices, and civil society and the media, respectively. External, independent, and public oversight are nevertheless united in that they are the responsibility of actors or institutions that fall outside of a service's chain of command.

1. Establishing a Comprehensive Legislative Basis for Effective Internal Control

Internal control systems translate abstract legal provisions into administrative and 'day-to-day' operational instructions. Thus, the starting point for establishing an effective internal control system is the development of a clear legislative mandate for intelligence services. Such a mandate can be composed of various laws,[9] which together should explicitly define the function and scope of powers of intelligence services, including the procedure for authorizing the use of special powers; the prohibition of certain activities; the retention and use of personal data; appointment processes; and the protection of whistle-blowers.

8 It should be noted that in certain countries within the Euro-Atlantic area, the heads (directors) of civilian and military intelligence services can also be members of joint executive bodies, such as the National Security Council in Croatia.

9 Such laws typically include a law that guides the work of the service, as well as laws that regulating the civil service and specialised legal provisions designed to safeguard civil liberties, such as data protection laws. For example, in Germany, the Federal Intelligence Service (Bundesnachrichtendienst – BND) is regulated by an overarching law which guides the work of the service, as well the law on the federal civil service, the federal budget regulation and the federal protection data law. See: https://www.gesetze-im-internet.de/bbg_2009/; https://www.gesetze-im-internet.de/bho/ and https://www.gesetze-im-internet.de/bdsg_2018/

Functions and powers

The functions and powers of intelligence services should be clearly defined in legislation. Intelligence services have exceptional powers. Legislation should therefore define the circumstances in which they can operate. These circumstances are usually limited to threats to national security and other serious threats such as terrorism. While the functions of intelligence services differ across countries, the collection, analysis, and dissemination of information relevant to the protection of national security is generally a core task performed by most intelligence services. As such, many states also prescribe legislative limits on the functions of intelligence services.

Authorizing the use of special powers

In Euro-Atlantic countries, legislation often defines the process for authorizing the use of special powers, such as the interception of communications, by intelligence services. In carrying out their work, intelligence services typically have powers that go beyond those of law enforcement services and have the potential to significantly undermine human rights and freedoms. The use of these powers should be proportionate to the security threat faced, and the process for authorizing these powers should reflect certain fundamental principles, including necessity and appropriateness, especially when human rights and freedoms are restricted.

Prohibition of certain activities

The special powers exercised by intelligence services are not unlimited, and certain activities – such as torture and cruel and degrading treatment – should be prohibited in all circumstances. The process for authorizing the use of special powers should be defined in legislation and draw on international norms and conventions such as the Geneva Conventions, the International Covenant on Civil and Political Rights, the UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, and the European Convention on Human Rights, among others.

Retention and use of data

Much of the work of intelligence services involves the collection and retention of vast amounts of data, including personal information. The inappropriate storage, dissemination, or disclosure of such material may have significant consequences for individuals in relation to their personal life, career, or safety. Legal frameworks should therefore provide the basis for the development of internal guidelines regulating the use and retention of data.

Standardized hiring process

The process for appointing intelligence service staff should, in so far as possible, be open and transparent. Internal guidelines and practices should be developed based on legislative provisions and norms that clearly prohibit political interference, nepotism, and cronyism in appointment processes, as well as other conflicts of interest. As far as possible – and subject to security clearances – appointments should be based on merit on the same basis as other administrative positions within the state.

Whistle-blower protection

At a minimum, legislation should refer to the protection of whistle-blowers. Such legislation should be translated into internal guidelines that provide protection for intelligence service staff who wish to report illegal activity or wrongdoing. This should involve processes that allow staff to report concerns internally, without the threat of retribution, as well as procedures for individuals to report concerns to external oversight bodies.

Table 1. Examples of whistle-blower legislation in Australia, New Zealand, and the United States

Country	Law	Description
Australia	Public Interest Disclosure Act 2013	• The Act includes provisions to allow current or former staff to report concerns to the Inspector-General of Intelligence and Security. • Intelligence services are required to respond to disclosures and report follow-up actions to the Inspector-General.
United States	Intelligence Community Whistleblower Protection Act 1998	• The Act includes provisions to allow staff and contractors to report issues of 'urgent concern' to an Inspector General of one of the US intelligence services, or directly to the House and Senate Select Committees on Intelligence. • The Act has a broad definition of what constitutes an 'urgent concern' that includes breaches of the law, false reporting to Congress, and action taken in reprisal against individuals who have reported concerns
New Zealand	Protected Disclosures Act 2000	• The Act includes guidelines for internal procedures on whistle-blowing protection. • It also includes provisions to allow intelligence service staff to report concerns to the Inspector-General of Intelligence and Security.

2. Key Components of an Internal Control System

Based on an analysis of several Euro-Atlantic countries, the following key components of an internal control system can be identified:

A code of values and/or ethics

A key aim of internal control is to develop a culture of compliance within an organization. Compliance here is understood as complying with an intelligence service's rules and norms, and abiding by certain principles, values, and ethical standards. The latter is commonly achieved through the development of a code of ethics and/or values. Values define what drives an organization's work, while a code of ethics defines the approach to how the work is carried out.

Intelligence services should define a set of values that they expect their staff to adhere to, such as integrity, respect, innovation, or excellence. These values should be fully endorsed by the senior management, with staff rewarded for demonstrating adherence. Services should also develop a code of ethics, which normally includes subjects such as honesty and respect for human rights principles and international law.

The combination of these two codes creates a culture of self-regulation and defines how staff should approach their work. This is especially important for issues that arise in so-called 'grey areas', where formal internal processes and legislation do not always provide clear guidance. These codes should be backed up by training (especially during induction) that clearly reinforces why it is important to adhere to them. In Euro-Atlantic countries, such as the United Kingdom, services also employ independent ethics counsellors to enable the organization to discuss ethics and values as well as advise the senior management.

Case study: The UK consolidated guidance for intelligence and service personnel on the treatment of detainees

Intelligence services may also employ other methods to develop a culture of compliance. These can take the form of guidance material on specific themes or issues. For example, in July 2010 the UK government published a short document entitled **Consolidated Guidance to Intelligence and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees.** It was published partly in response to a civil suit brought by a UK citizen who had been held at Guantanamo Bay. Inquiries by the Intelligence and Security Committee of Parliament

had also revealed that UK intelligence agency personnel deployed to Afghanistan and Guantanamo Bay were not sufficiently trained on the Geneva Convention and were unaware that certain interrogation techniques had been specifically banned by the UK government in 1972.

The **Consolidated Guidance** drew on a range of existing documents, including separate policy documents produced by each of the intelligence and security services, as well as established military doctrine. It brought together in a single document the key principles – consistent with the UK's obligations under domestic and international law – governing the treatment of detainees abroad and the exchange of intelligence with liaison countries relating to detainees. It obligated all intelligence staff to consider the risk of detainees being subjected to torture or other cruel, inhuman, or degrading treatment and provided a system for reporting any serious risk of torture or mistreatment to senior staff and, in some cases, government ministers.

The **Consolidated Guidance** is a rare but significant example of a published internal guidance document governing the actions of UK intelligence personnel. It represented a significant advance in transparency and was clearly designed to reassure the British public that the services operate within the law. Although the **Consolidated Guidance** does not stand alone and working-level, unpublished guidance continues to be applied within the services, it has provided an element of consistency regarding the responsibilities of UK intelligence and military personnel that had not previously existed.

Moreover, the guidance was reviewed before publication by the UK parliament's Intelligence and Security Committee, and following publication was subject to further scrutiny by the committee and a number of NGOs. As a result of concerns raised through these channels, revised guidance was published in 2011. The implementation of the guidance continues to be monitored by the parliamentary committee and the judicial commissioner responsible for the intelligence services, both of which publish reports that have, for example, examined several cases in detail and outlined the number of times that concerns about possible mistreatment have been referred to ministers.

Standardized operating procedures

Every intelligence service should develop standard operating procedures (SOPs), which provide an important basis for internal controls and audits. All investigations and operations within a service should follow the same basic SOPs. While procedures vary from service to service, they normally include basic SOPs for initiating and conducting operations or investigations. Although each

operation is different, standard SOPs should exist for conducting technical, intelligence (human sources), and surveillance operations. SOPs should state how operations are to be conducted and which methodologies will be used. Legal and ethical compliance is a key component of the SOPs. Prior to authorizing an operation, services should develop an internal 'checklist' to examine the legal and ethical implications of a given operation or investigation. Such a checklist might include the following:

- the reason for the initiation of the operation or investigation, and its link to national intelligence priorities;
- the operation's goals;
- the person and/or post who is responsible for the operation;
- potential security risks and mitigation strategies;
- legal issues (such as judicial warrants or compliance with legislation);
- political considerations (such as the risk to international relations);
- stakeholders who should be consulted;
- other compliance issues (such as ethical and health and safety issues); and
- when the operation or investigation should be reviewed.

Clear lines of responsibility

Ensuring clear lines of responsibility within an intelligence service is key to ensuring that audits are objective; to preventing self-tasking and the politicization of services; and to enhancing internal accountability for decision making.

Managers should be informed of their responsibilities and the scope of their powers. This is especially important for operations. Best practice dictates that those conducting operations should be separated from those responsible for authorizing them so as to ensure that audits of operations are as objective as possible. This division of responsibilities also acts as a safeguard against self-tasking or unscrupulous political executives tasking services for their own ends. This allows security clearance applications to be processed more effectively as decisions are made independently of the team pursuing the operational goal. It also enables the senior management to record additional permissions in writing where necessary – thereby clearly identifying who is responsible for any action and allowing them to be held accountable.

Professional legal guidance

Timely and practical legal advice is critical to ensuring intelligence efforts stay within legal, procedural, and ethical boundaries. While many countries have an extensive array of laws governing the work of the services, they cannot account for all possible scenarios. Equally, operational staff may not be fully aware of all aspects of legislation covering issues as diverse as criminal law and human rights. As such, services sometimes employ legal advisers (who are not accountable to the operational staff) to advise the services. In some countries in the Euro-Atlantic area, such as the United Kingdom, services have begun embedding legal advisers in specific operational departments in an effort to sensitize them to the work and goals of the department in question and to enhance the staff's understanding of legal constraints and considerations. This is particularly common in departments dealing with counterterrorism.

Proper induction and training

As with all organizations, induction and regular training significantly impacts the service's effectiveness. Poor or inadequate induction training can undermine staff performance and increase the risk of misconduct or unacceptable behaviour. Staff should receive training on the organization's official procedures and their importance; it is much easier to achieve a desired working culture within the service if these procedures are understood early on. It is also important that staff not only understand how operations work but also have an appreciation of the wider context and why such operations are carried out.

Staff also need to be made aware early in their careers, however, that they are responsible for their actions; they should be informed of the potential consequences of not following processes put in place to safeguard the work of the service and understand actions that could have adverse consequences for an individual(s) either within or outside the service.

Vetting and security procedures

All intelligence services should have clear procedures for vetting and issuing security clearances for staff. This not only protects national security but also helps to ensure that staff working in the service have the appropriate attitude towards compliance and the service's work. Even if they are loyal to the organization and its goals, staff members who fail to follow the rules or respect the rights of individuals should have their security clearances removed.

It is also important for operational security staff to work alongside

operational teams to ensure that operations do not compromise the safety or livelihood of the individuals working on that operation – be they staff, intelligence sources, or members of the public.

Senior management support for compliance

Senior management should fully support the organization's internal control procedures and promote compliance. This is critical to ensure that mid-level management and staff follow the rules and abide by the service's proper procedures. Rigorous appointment procedures should also be in place for those in senior management as they are responsible for individuals under their control, as well as for activities (that is, operations, measures, and decisions) implemented under their authority. In the United Kingdom, the Nolan Principles – which outline the expected behaviour of public officials – are central in determining an individual's suitability to hold a senior public position. Furthermore, the performance of senior managers should be measured according to their level of adherence to the correct behaviour and attitude.

Internal communication tools

Like any organization, intelligence services should use internal communications to promote internal control and good governance. Effective communication should clearly inform staff of internal procedures and expectations. This serves to reinforce internal control procedures and can be achieved through an internal intranet, thus reducing the risk of misinformation. Equally, good external communications provide the public with information about external and internal control procedures within the organization. Internal communications systems should be used as a method for staff to provide feedback to management.

Comprehensive record-keeping

It is essential that all activities and decisions made by an intelligence service are recorded in a consistent and detailed manner. Investigation or operation records should include the same information: why the operation was started; whether all the appropriate considerations were made before beginning the operation; the operation's progress; any key decision points; and reviews of the operation. A consistent approach to record-keeping also serves as an important reminder to staff to follow all the compliance measures.

Establishment of a formal internal control body

A fundamental instrument of internal control consists of a formal organizational body responsible for systemically preventing, investigating, and reporting on unlawful or unethical behaviour.

Such bodies usually have systemic responsibilities and special authority, and act on behalf of the highest levels of authority (that is, the president, executive government, or director). Some services, such as those in the United States, have an Inspector General. Others appoint a deputy or assistant director responsible for internal control. Croatia's Security and Intelligence Agency (SOA), for example, has a department headed by an assistant director responsible for internal control, including for investigating complaints, improper activities, and other disciplinary issues.

3. Challenges to Internal Control

The previous section outlined the common components of internal control systems in intelligence services. These components have been developed in response to particular challenges faced by intelligence services in ensuring effective internal control. These challenges include adapting training regimes to changes in legal frameworks; balancing control with operational effectiveness; controlling the use of advanced technologies; and addressing the issue of the so-called 'Esprit de Corps' versus the 'code of silence'. The section below examines these challenges using the German Federal Intelligence Service (Bundesnachrichtendienst, BND) as a case study.[10]

Adapting training regimes to changes in legal frameworks

To remain effective, internal control requires regular training, not only to familiarize staff who have been promoted with their new responsibilities but also to ensure that managers with control responsibilities receive up-to-date training. This is necessary because intelligence requirements and methods are evolving and internal control mechanisms need to be adapted accordingly, and because the legal landscape within which an intelligence service operates is also constantly evolving.

For example, in 2020 the German Federal Constitutional Court passed a landmark decision regarding electronic surveillance of the BND outside Germany.[11] It declared that certain provisions concerning electronic surveillance in the BND law of 2016 were not compatible with the German constitution and asked the federal government to make appropriate changes.[12] The decision was based on the finding

10 It should be noted that these are general challenges and may also apply to contexts other than the German intelligence services.

11 Federal Constitutional Court (Bundesverfassungsgerichts). 2020. 'Leitsätze zum Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17'. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html.

12 This led the Federal Government to suggest changes to the BND law, which was passed in July 2021. See: Federal Intelligence Services Act (Gesetz über den

that fundamental rights enshrined in the German constitution are not limited to the jurisdiction of German citizens but also extend to German government authorities, such as the BND. These authorities must therefore respect these fundamental rights in all cases. The court ruled that the reasons for foreign electronic surveillance must be better defined and safeguards against aimless blanket surveillance need to be strengthened.[13]

This ruling has obviously significantly impacted internal control mechanisms, which now need to facilitate oversight of the BND's implementation of the court's decision in its day-to-day work. Changes in the legal environment –– whether due to the passing of new laws or the interpretation of laws by the courts – will always require the adjustment and further fine-tuning of internal control mechanisms.

Balance between control and operational effectiveness

Regarding the delegation of responsibilities to lower levels of authority, a balance has to be struck in order to ensure operational efficiency. As more authority is delegated to lower levels of management, there is less effective control by senior management. On the other hand, if senior management attempt to centralize authority and delegate fewer responsibilities to lower levels of authority, this can negatively affect operational dynamics (including flexibility and adaptability). Given the complex nature of human intelligence (HUMINT) and signals intelligence (SIGINT) operations, maintaining the ability to react quickly to changing circumstances is crucial for effective intelligence gathering. For example, in 2012, shortly after his appointment as the new president of the BND, Gerhart Schindler criticized the service for being hampered by too many bureaucratic hurdles.[14] It is, however, impossible to define concrete standards to achieve this balance as they depend on the particular legal environment, mandate, and working methods of each service. Indicators that require approval and control from higher levels of the hierarchical chain include the size, complexity, and strategic importance of an operation; risk levels, which need to be defined beforehand; and budget implications.

Bundesnachrichtendienst, BNDG). Available at: https://www.gesetze-im-internet.de/bndg/BJNR029790990.html.

13 Federal Constitutional Court (Bundesverfassungsgerichts). 2020. 'Ausland-Ausland-Fernmeldeaufklärung nach dem BND-Gesetz verstößt in derzeitiger Form gegen Grundrechte des Grundgesetzes'. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2020/bvg20-037.html.

14 Die Welt. 2012. 'Paradigmenwechsel beim Bundesnachrichtendienst'. Available at: https://www.welt.de/politik/deutschland/article108564662/Paradigmenwechsel-beim-Bundesnachrichtendienst.html.

Controlling the use of advanced technologies

Given the increasing use of sophisticated technologies such as machine learning and artificial intelligence, the level of complexity of technical surveillance and monitoring systems is growing rapidly. These sophisticated technologies, coupled with the increasing use of online services, allow for far greater intrusiveness through electronic surveillance. Ensuring that the use of such technologies does not unduly infringe upon others' rights and basic freedoms presents a significant challenge for internal control mechanisms. Consequently, controls by design rather than ex post facto are becoming the common means through which to approach this issue.[15]

The so-called BND-NSA affair in Germany in 2015 highlights the complexity of internal control in an era of ever-increasing technological developments. This incident, which was the subject of extensive parliamentary inquiries, refers to joint electronic surveillance by the BND and the US National Security Agency (NSA) of electronic communications in the Middle East and North Africa (MENA) region via a surveillance station in Germany.[16] At the core of this complex incident was the question of whether the BND sufficiently checked so-called 'selectors' that were being transmitted to the NSA on a weekly basis.[17] These selectors also included German, European, and NATO-partner targets operating in the MENA region. Surveillance of such targets – particularly that of German citizens, companies, or institutions – is subject to extremely strict controls and judicial permissions and is usually outside the legal mandate of the BND. It became clear that the internal checks of these selectors within the BND and the corresponding internal control mechanisms had not functioned properly.[18] This demonstrates the challenges of internal control when dealing with mass data. The incident led to significant

15 For a range of recommendations, see for example: Stiftung Neue Verantwortung. 2019. Data-driven Intelligence Oversight: Recommendations for a System Update (Berlin: Stiftung Neue Verantwortung). Available at: https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf.

16 Deutsche Welle. 2015. 'The BND affair: "No better partner than the USA"'. Available at: https://www.dw.com/en/the-bnd-affair-no-better-partner-than-the-usa/a-18407523.

17 'Selectors' are data points such as telephone numbers, email addresses, IP addresses, names, or keywords. See: Der Spiegel. 2015. 'German Intelligence Under Fire for NSA Cooperation'. Available at: https://www.spiegel.de/international/germany/german-intelligence-agency-bnd-under-fire-for-nsa-cooperation-a-1030593.html.

18 netzpolitik.org. 2016. 'Der BND bricht dutzendfach Gesetz und Verfassung – allein in Bad Aibling'. Available at: https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/# Sachstandsbericht.

adjustments in internal BND control mechanisms[19] and a new version of the BND law in 2016.[20]

'Esprit de Corps' versus 'code of silence'

The specific responsibilities of members of intelligence services and restrictions owing to the sensitivity of their work tend to foster a strong sense of community or 'esprit de corps'. This cooperative spirit is of course a motivating factor and necessary for the service to function effectively. It can also, however, be an inhibiting factor for internal control mechanisms as problems or mistakes may not be reported appropriately or in a timely fashion.

Recent investigations into potential right-wing extremist tendencies in German military, police, and intelligence forces highlighted this issue.[21] One of the core challenges identified was 'insufficiently effective' internal reporting of incidences.[22] For example, the internal control mechanisms of the German military special forces, the Kommando Spezialkräfte (KSK), were found to be particularly inadequate. Consequently, the German ministry of defence, which oversees the KSK, outlined a range of reforms, the basic tenets of which are also relevant to the challenges encountered by internal control systems of intelligence services. One key measure involved irregularly rotating officers into and out of the KSK to ensure they are able to oversee the force effectively and not hampered by undue personal relationships to the soldiers.[23] Consequently, an appropriate balance should be found between the development of specialized knowledge, including at the managerial level, within units that require a significant level of expertise in a particular area, with the need to regularly move managerial staff between units to ensure effective internal control.

19 Federal Government (Bundesregierung). 2016. 'Klare Regeln für Auslandsaufklärung'. Available at: https://www.bundesregierung.de/breg-de/aktuelles/klare-regeln-fuer-auslandsaufklaerung-435766.

20 The BND-law changed again in 2021 following the ruling of the German Federal Constitutional Court. See: Deutschlandfunk. 2016. 'Geheimdienst-Reform: Bundestag beschließt umstrittenes BND-Gesetz'. Available at: https://www.deutschlandfunk.de/geheimdienst-reform-bundestag-beschliesst-umstrittenes-bnd.1766.de.html?dram:article_id=369171.

21 Bundesamt für Verfassungsschutz. 2020. Rechtsextremisten in Sicherheitsbehörden: Lagebericht. Available at: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/2020/lagebericht-rechtsextremisten-in-sicherheitsbehoerden.pdf?__blob=publicationFile&v=7.

22 See for example: Der Spiegel. 2020. '"Die Mauer des Schweigens bröckelt"'. Available at: https://www.spiegel.de/politik/deutschland/rechtsextreme-im-ksk-die-mauer-des-schweigens-broeckelt-a-06c33e4f-d93c-4116-976e-9774ad9fea9d.

23 Federal Ministry of Defence (Bundesministerium der Verteidigung). 2020. 'KSK-Reform: Weitere Maßnahmen im Einzelnen'. Available at: https://www.bmvg.de/de/aktuelles/ksk-reform-weitere-massnahmen-273602.

Recommendations

Considering the aforementioned challenges and key components of internal control systems, the following recommendations can be made to strengthen internal control:

- **Develop a code of ethics and values:** Independent ethics counsellors should support services with the development of a code of ethics and values; this code should be reinforced through regular training. Where necessary, and in collaboration with external oversight and control bodies, services may also develop subject-specific ethical guidance material, for example on detention regimes or the use of intrusive surveillance measures.
- **Create standardized operating procedures (SOPs):** SOPs should be developed for initiating and conducting operations or investigations. These should be further tailored to technical, intelligence (human sources), and surveillance operations. They should include a rigorous checklist that includes an examination of the legal and ethical implications of a given operation or investigation.
- **Ensure clear lines of responsibility:** Those conducting operations should be separated from those responsible for authorizing them; managers should also be informed made aware of their exact responsibilities and roles. This serves to prevent self-tasking and the politicization of services; to enhance internal accountability for decision making; and to ensure that audits are objective.
- **Provide professional legal guidance:** Legal advisers should be embedded within intelligence services. Units or departments responsible for operations with potentially serious ethical or legal implications should have their own legal advisers.
- **Organize induction and regular training:** All staff should receive training on the official procedures of the organization, why these procedures are important, and the expected behavioural norms of the intelligence service. Such training should be provided to all new staff and repeated on a regular basis.
- **Link vetting and security clearances to internal control requirements:** Intelligence service staff who fail to follow internal control requirements or respect the rights of individuals should have their security clearances removed.
- **Lead by example:** Senior management should strictly follow internal control guidelines. This can be facilitated by developing

a normative set of principles that guides the behaviour of public sector officials, such as the UK's Nolan Principles.

- **Ensure effective internal communication:** Internal communication tools should be developed to inform staff of all compliance and internal procedures.
- **Provide for comprehensive record-keeping:** All the activities and decisions made by an intelligence service should be recorded in a consistent and detailed manner. This ensures accountability for decision making and enhances the effectiveness of ex post reviews.
- **Establish and build the capacity of formal internal control bodies:** All intelligence services have internal control bodies. Such bodies are generally responsible for internal financial control, as well as for preventing, investigating, and reporting on unlawful or unethical behaviour. In general, they should have systemic responsibilities and special authority, and act on behalf of the highest levels of authority (that is, the president, executive government, or director). They should also provide regular training for intelligence staff. Clear procedures and SOPs related to their activities need to be constantly updated to adapt to changing realities.

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

www.dcaf.ch

@DCAF_Geneva