DCAF Geneva Centre for Security Sector Governance

SSR BACKGROUNDER

INTELLIGENCE OVERSIGHT IN THE AGE OF DIGITALIZATION

ABOUT THIS SSR BACKGROUNDER

This Backgrounder examines the impact of digitalization on the work of the intelligence services and underscores the importance of democratic intelligence oversight in the context of digitalization. While digital technologies enable intelligence services to produce credible intelligence, they also challenge issue areas such as privacy, human rights, transparency, data management, safety, and accountability. Intelligence oversight bodies lack the requisite capacity to effectively scrutinize the impact of the use of digital technologies by intelligence services in these fields. Therefore, overseers must not only have a legal mandate but also the digital capabilities and expertise to incredibly oversee a continuously evolving spectrum of the digital practices of intelligence services. This Backgrounder outlines how good security sector governance (SSG) can strengthen democratic oversight of intelligence services under the new challenges posed by digitalization.

THIS SSR BACKGROUNDER ANSWERS THE FOLLOWING QUESTIONS:

Why is democratic intelligence oversight relevant in the context of digitalization? . . . 2
How does digitalization impact the work of intelligence services? . . . 4
How does digitalization impact the role of intelligence oversight actors? . . . 5
What are the challenges and opportunities of digitalization in the oversight of intelligence services? . . . 6
How can good SSG strengthen democratic oversight of intelligence services in the context of digitalization? . . . 7

ABOUT THIS SERIES

The SSR Backgrounders provide concise introductions to topics and concepts in good security sector governance (SSG) and security sector reform (SSR). The series summarizes current debates, explains key terms and exposes central tensions based on a broad range of international experiences. The SSR Backgrounders do not promote specific models, policies or proposals for good governance or reform but do provide further resources that will allow readers to extend their knowledge on each topic.

The SSR Backgrounders are a resource for security governance and reform stakeholders seeking to understand and also to critically assess current approaches to good SSG and SSR.

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 wishes to thank
Sondra Cheong for research, conceptualization and authorship. Nathalie Gendre, Jean-Michel Rousseau, and Gabriela Manea for peer review and comments. David Wilson for copy editing in English. Petra Gurtner for layout and design.

This SSR Backgrounder was developed in collaboration with the Master of Advanced Studies in European and International Governance (MEIG) of the University of Geneva.

MEIG MASTER OF ADVANCED STUDIES EUROPEAN AND INTERNATIONAL GOVERNANCE

Series Editor
Gabriela Manea

To cite this publication
DCAF – Geneva Centre for Security Sector Governance. Intelligence Oversight in the Age of Digitalization. SSR Backgrounder Series. Geneva: DCAF, 2024.

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

info@dcaf.ch
+41 22 730 94 00

www.dcaf.ch

WHY IS DEMOCRATIC INTELLIGENCE OVERSIGHT RELEVANT IN THE CONTEXT OF DIGITALIZATION?

Digitalization has transformed the way in which intelligence services gather and produce intelligence informing national security decisions. By design, the work of intelligence services is covert, secret, and classified, and is often undertaken using intrusive methods of information gathering, which due to digitalization are becoming increasingly sophisticated.

For instance, artificial intelligence (AI) and machine learning (ML) give intelligence services access to larger volumes of data, producing intelligence, solving problems, and analysing threats in a timely manner. However, this trend challenges issue areas such as privacy, human rights, transparency, data management, safety, and accountability.

→ For further information, see the SSR Backgrounder on Digitalization and Security Sector Governance and Reform.

While the nature of intelligence services makes overseeing them difficult, it is vitally important that they are subject to robust oversight. In the absence of effective democratic intelligence oversight, digital technologies can be used to surveil citizens, control free expression, and censor information. They can also be used by national and foreign intelligence services to manipulate political decisions and electoral processes. These actions undermine democratic values and good SSG.

→ For further information, see the SSR Backgrounder on Security Sector Governance.

Democratic intelligence oversight is relevant because:

- It lays down a clear legal framework which defines the mandates of intelligence services, including specific areas of responsibility, limits, and methods for information gathering.
- It provides oversight bodies with the mandate and power to credibly assess the performance of intelligence services, ensuring access, independence, discretion, and authority.
- It ensures compliance with their legal mandate and, thereby, respect for democratic governance, rule of law, and gender equality.
- It protects against political abuse by building merit-based and professional intelligence services.
- It bolsters the legitimacy, integrity, and effectiveness of intelligence services as accountability leads to greater transparency and more trust by policymakers and the public in their work. This is important in order to secure political and public support for resource allocation to increase the response capacities of intelligence services to new and emerging security challenges resulting from digitalization.

→ For further information, see the SSR Backgrounder on Intelligence Oversight.

.

DEFINITION OF DIGITAL TERMS AND CONCEPTS

Advanced analytics: **a** variety of of data analytics techniques, such as machine learning, that are employed by businesses and other organizations to improve their decision-making.

Artificial intelligence (AI): machines or devices that have software that learns from experience, adjusts to new inputs, and performs human-like tasks.

Augmented intelligence analysis: combines AI and machine learning with human judgement and decision-making.

Behavioural analytics: uses AI and big data analytics on user behavioural data to identify patterns, trends, anomalies, and insights into the behaviour of customers on digital platforms such as websites, email, and mobile apps.

Blockchain technology: **a** shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.

Cloud computing: delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the internet ('the cloud') to offer faster innovation, flexible resources, and economies of scale.

Cognitive automation: uses automation technologies such as AI to streamline and scale decision-making across organizations to improve operational efficiencies.

Deep learning: **a** subset of machine learning which makes complex correlations between data and learns from examples and previous mistakes. It requires larger amounts of data compared with machine learning.

Digitalization: technical process of converting and storing text, pictures, and sounds in a digital format, describing data transition from an analogue to a digital format.

Machine learning (ML): discipline of AI which helps machines to imitate intelligent human behaviour, teaching computers to learn from data, identify patterns, and make predictions on their own.

Principle of 'explainability' of AI: **a** set of processes and methods that allow human users to comprehend and trust the results and output created by machine learning algorithms.

FIGURE 1 RISKS ASSOCIATED WITH ARTIFICIAL INTELLIGENCE

HOW DOES DIGITALIZATION IMPACT THE WORK OF INTELLIGENCE SERVICES?

Intelligence services are primarily responsible for providing governments with credible information about possible threats to the state and its population. They define and develop coherent national security and military strategies and policies and prevent threats to national security. Additionally, intelligence services are engaged in defensive and offensive counterintelligence, as well as covert actions, also known as special political actions.

→ For further information, see the SSR Backgrounder on Intelligence Services.

Digitalization has provided opportunities for the modernization of intelligence services, relative to their scope of mission and the pace at which intelligence is produced. While digitalization is a relatively new phenomenon as compared with the work of intelligence services, it has transformed key activities such as intelligence collection, processing, and analysis.

With digital technologies, the role of intelligence services has been enhanced, particularly in their capacity to produce credible information and divert threats to national security, such as cybersecurity, terrorism, cyber espionage, disinformation, biotechnology, etc. Technological democratization and globalization have also empowered individuals and groups, whether or not working for states, as well as foreign state actors, to exploit tech-enabled intelligence tools to carry out activities undetected, such as cyberattacks, hacking, installation of malware, and theft of sensitive data. This complicates the global security environment and requires intelligence services to invest in newer technologies to remain one step ahead.

To counter these threats, intelligence services have adapted by using surveillance and machine learning technologies in intelligence analysis and biometric identification, although the extent to which digital technologies are applied is not known due to the secretive nature of intelligence activities.

Collection

Technologies such as AI and ML, cloud computing, and advanced analytics have enhanced the capability of intelligence services to collect data from a wide range of digital sources. AI is applied in some cases in automating aerial reconnaissance, surveillance, and target monitoring, while ML algorithms are used to verify and validate targets collected from images. Moreover, surveillance activities have moved beyond data gathering and involve real-time monitoring of online activity.

However, information collection is no longer solely the domain of the intelligence services. Private corporations, including private military and security companies (PMSCs), as owners and drivers of emerging technologies engage in mass surveillance, digital profiling of citizens, and behavioural modification, made possible through the commercialization of space and proliferation of satellite-based imaging and sensors. This infringes on human rights and the state's authority to engage in intelligence production and has serious ethical and security implications because the activities of private corporations in this domain are not subject to strong regulatory control and oversight.

Processing

AI enhances the filtering of large volumes of data and information used for making intelligence-based decisions. AI is used to identify patterns in data and to identify anomalies that might otherwise be difficult for human intelligence officers to detect and has been deployed to process and automate information collected from satellites and aerial intelligence, surveillance, and reconnaissance data.

However, the processing of information has become challenging due to the mass volume of digitized information, which is complicated by the fast pace at which misinformation and disinformation are spread across the multitude of social media platforms. This is testing the processing capabilities of the intelligence services and will require them to adopt a more diligent and thorough approach in detecting and filtering incorrect information that can otherwise have negative consequences on analysis and decision-making.

FIGURE 2 KEY ACTIVITIES OF INTELLIGENCE GATHERING

Analysis

The intelligence services rely on 'AI-augmented intelligence' to analyse information, using tools such as cognitive automation and behavioural analytics. These tools have become increasingly used and even replaced tasks such as language processing, facial matching, transcription of text from audio, and fraud detection, which were traditionally performed by human analysts. Some intelligence services have also started using deep learning to boost the efficiency and effectiveness of analysts.

Analysts are required to learn new skillsets to measure the authenticity of data in their analysis and increase their awareness of the principle of 'explainability' of AI, which allows decision-makers to provide a rationale for a given decision. These skillsets give analysts the ability to detect limitations in the use of technologies and to understand the logic, assumptions, and data biases of AI. While this is encouraging, digitalization will continue to create a dependency on digital technologies, thereby eroding human intuition in analysis and decision-making. Moreover, AI presents risks in perpetuating social biases linked to gender, race, and ethnicity throughout the lifecycle of intelligence production, for instance with the use of facial or speech recognition software.

HOW DOES DIGITALIZATION IMPACT THE ROLE OF INTELLIGENCE OVERSIGHT ACTORS?

In a democratic system of government, oversight of the intelligence services involves the executive, judiciary, and legislative branches of government, internal control within intelligence services, and independent and public/informal institutions, including civil society and media.

→ For further information on intelligence oversight actors, see the SSR Backgrounder on Intelligence Oversight.

Digitalization **enhances the efficiency of intelligence oversight actors:**

- Communication platforms such as websites and social media can enable intelligence oversight actors to reach a wider audience in keeping the public informed about their activities.
- Parliamentary and budget-related debates, commissions of inquiry, committee briefings, etc., can now be streamed live on online platforms, allowing for real-time engagement with the public. Due to increased internet connectivity, formal and informal oversight actors can collect information on human rights violations from places that were once inaccessible.
- Civil society can use available digital platforms to shape laws and policies through information sharing, public consultations, expression of views, mobilization of campaigns and protests, and collection of funds.

However, intelligence oversight actors often lack the requisite capacity to effectively scrutinize problematic areas, such as data privacy, protection, and sharing; potential human rights abuses and discrimination in the digital space; and digital security risks. Overall, intelligence oversight actors receive less support to keep up with digital technologies compared with intelligence services. Moreover, digital technologies such as AI are not subject to public scrutiny, falling under the category of trade secrets.

Digitalization is also testing the limits of existing laws and regulations pertaining to political engagement as it directly impacts freedoms of expression, association, and assembly and access to information. Some governments have been forced to amend their legislation to cater for data protection and digital security, and to establish initiatives aimed at strengthening the role of civil society to promote transparency. However, there remains ambiguity on how emerging technologies such as AI are developed and deployed, which makes it challenging to establish proper oversight and accountability mechanisms.

Intelligence oversight actors must:

- have the highest level of access to personnel, sites, and classified information. Accordingly, schedules for the classification of information and laws on freedom of information should favour access to such information **(Access).**
- be independent of political interests and inappropriate influence by intelligence services. Dedicated budgets and expert personnel help to guarantee credible oversight **(Independence).**
- be designed to maintain secrecy and the integrity of the intelligence process. Reliability is necessary to win the confidence of the intelligence services to safeguard national interests **(Discretion).**
- have discretionary powers of investigation, including the power to compel testimony under oath. Special courts or judges must be dedicated to intelligence oversight **(Authority).**

→ For further information, see the SSR Backgrounder on Intelligence Oversight.

WHAT ARE THE CHALLENGES AND OPPORTUNITIES OF DIGITALIZATION IN THE OVERSIGHT OF INTELLIGENCE SERVICES?

Typical challenges to democratic oversight of intelligence services stem either from within the intelligence services themselves (internal) or from the context in which they operate (external).

→ For further information on challenges, please refer to the SSR Backgrounder on Intelligence Oversight.

FIGURE 3 INTERNAL CHALLENGES AND OPPORTUNITIES

CHALLENGES	OPPORTUNITIES
(1) Secrecy	
• Digital technologies reinforce the veil of secrecy of intelligence services, enabling them to potentially violate privacy in the name of national security. • Secrecy dilutes the intelligence oversight process, leaving the quality of oversight almost entirely dependent on the good will of the intelligence services, thereby undermining liberal democracies. • Digital technologies make it easier for authoritarian regimes to abuse fundamental rights of their own of and foreign citizens.	• Update the mandates of oversight institutions to oversee the use of digital technologies by intelligence services and strengthen their access to secret information. • Empower civil society to play a greater role in shaping policies on intelligence work and data policy. • Shed light on the activities of the intelligence services through investigative journalism and media coverage. • Enhance the use of digital technologies to empower oversight bodies and the public to access information.
(2) Discretionary authority	
• Intelligence professionals commonly have the discretionary power to make independent decisions. In the absence of an appropriate 'explainability' mechanism and rules of engagement, AI blurs the burden of responsibility in intelligence decision-making. • AI systems are often biased in terms of both gender and ethnicity, feeding wrong information into AI-generated decisions. This raises ethical challenges and requires more capacity and resources for oversight bodies, to uncover and counter such trends in the work of intelligence services.	• To ensure responsible independent decision-making, the management of intelligence services must instil at every level a culture of professionalism based on respect for good governance and the rule of law, including gender equality. • AI and emerging technologies must be designed in ways compatible with human rights at all stages of intelligence production.
(3) Exaggerated threat perceptions	
• Threats such as cybersecurity, terrorism, cyber espionage, and misinformation can justify a potentially abusive and excessive use of technologies such as AI, facial recognition, and drone surveillance, harming good SSG, human rights, and rule of law. • There are no redressal mechanisms for human rights violations through digitally informed intelligence practices, and no protection regime for whistle-blowers uncovering abuses.	• Strengthen professionalism and political independence, ensuring that intelligence analysis does not either over- or underestimate threats to national security, and refrain from human rights violations. • Develop a legal definition of intrusion and criteria for non-abusive data collection and analysis.

FIGURE 4 EXTERNAL CHALLENGES AND OPPORTUNITIES

CHALLENGES	OPPORTUNITIES
(1) Political will	
• The prioritization of other national security interests over the accountability of intelligence services has led to under-investment in legislative or executive oversight of such services, which is in stark contrast with the massive investment made by both governments and private sector companies in developing sophisticated technologies to carry out intelligence collection and surveillance. • The intrusiveness of surveillance technologies leads to public mistrust in the effectiveness of oversight bodies to protect human rights against problematic practices of intelligence services. • In the absence of effective oversight, the intelligence services can become subject to political manipulation, and vice versa.	• Develop holistic approaches that ensure enhanced oversight through greater collaboration between oversight bodies, government, and the private sector. • Protect intelligence services from political manipulation, by clearly defining the chains of political responsibility for decision-makers.
(2) International scope	
• Digitalization has made international intelligence cooperation pervasive and less subject to oversight. • Intelligence oversight bodies lack the knowledge and review mechanisms to ascertain whether and how national intelligence agencies share data with foreign intelligence agencies. This can result in accountability gaps, limitations on the effective review of data sharing, collusion, and democratic deficits at the international level.	• To prevent abuses and bolster the credibility of national intelligence services, new or existing laws and regulations must define the scope and nature of international intelligence cooperation and responsibility sharing.
(3) Technological developments	
• While technological innovation has empowered intelligence services, intelligence oversight bodies have been slow to benefit from technological advances, a mismatch resulting in adaptability, accountability, and transparency gaps.	• Incorporate enhanced digital expertise within the oversight bodies. • Keep legal frameworks up to date with digital developments. • For both, governments must invest in human and capacity building and in technologies tailored to the needs of oversight bodies.

HOW CAN GOOD SSG STRENGTHEN DEMOCRATIC OVERSIGHT OF THE INTELLIGENCE SERVICE IN THE CONTEXT OF DIGITALIZATION?

Undoubtedly, digitalization enhances the effectiveness and efficiency of intelligence services, but arguably this comes at a high cost. To counter potential negative impacts, the use of digital tools and technologies by the intelligence services must be subject to democratic principles and must have respect for fundamental values and human rights. Furthermore, the principles of good SSG (see Figure 3) must inform intelligence oversight.

Effectiveness and efficiency

- Intelligence analysts, as well as oversight actors, must be trained in ethics, transparency, and accountability, within the context of digitalization and emerging technologies.

- The executive oversight must match their investment (political, financial, and technical) in intelligence oversight with investment in uplifting the digital capabilities of the intelligence services.

- Since modern intelligence is data-driven, its oversight should be as well. As such, oversight bodies need to adopt tech-enabled instruments to respond to the technological advances driving the intelligence field.

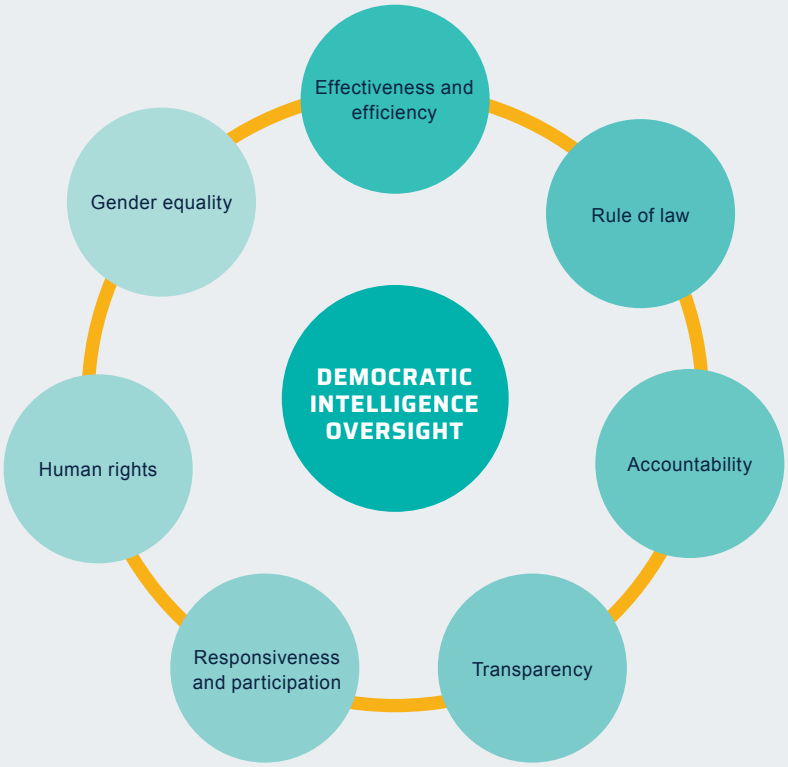
Rule of law

- Future technological innovation must take place within a clearly defined regulatory framework – for both intelligence services and private companies – that establishes justifiable, necessary, and proportionate criteria for information and data collection, processing, and analysis, which guarantee both the respect of individual rights and the necessary protection of intelligence activities.

- Tech companies and algorithmic decision-making must be subject to good governance through mechanisms which cater for algorithmic accountability, including the explainability of AI, and the availability of open-source code.

- Laws, policies, and budgets related to the intelligence services must be subject to scrutiny, to the extent that this does not threaten national security. Formal and informal oversight bodies must be designed so as to render intelligence services 'overseeable'.

FIGURE 5 DEMOCRATIC INTELLIGENCE OVERSIGHT AND PRINCIPLES OF GOOD SSG



- Privacy and data protection laws should not provide wide exemptions for intelligence services.

- The executive, legislative, and judiciary must ensure a viable system of checks and balances and guarantee the political independence of intelligence services.

Accountability

- Oversight bodies must conduct assessments on emerging technologies to ensure that human rights, including non-discrimination, respect of privacy, and gender equality are respected in the operations of intelligence services, and most importantly in the development and deployment of digital tools by private companies. Intelligence oversight bodies must also adhere to these principles when using digital tools in their activities.

- An ethics-based auditing system must be established that will require intelligence services to explain and justify their decisions, including those made by AI, and especially any potentially severe consequences of these decisions.

- Internal control and senior management within intelligence services must reinforce accountability by establishing rules and procedures to ensure that staff act professionally and effectively within the limits of their authority, in compliance with the law, human rights, and gender equality. Mechanisms for sanctioning illegal action, redress for victims of such abuses, and whistle-blower protection must be put in place. The judiciary must carefully monitor the practice of special powers, adjudicate on charges of misconduct levelled against members of the intelligence services, and prosecute possible misconduct.

- A conducive environment must be created for civil society to report wrongdoing and to access remedy in such situations. The media must also play a greater role in undertaking investigative journalism to expose any wrongdoings by the intelligence services and to hold them publicly accountable.

Transparency

- A legal framework must be established which clearly defines the mandates, roles, responsibilities, and limits of the intelligence services as well as of oversight bodies.

- Oversight bodies must continuously engage the intelligence services to build trust in accessing and reviewing operational systems, as well as scrutinizing data collection and analysis systems in an accurate and timely manner.

- The intelligence services must work closely with private developers of digital technologies to ensure that data is collected solely for its intended purposes and in a safe manner, in keeping with the rule of law and human rights, and with no threat to human or national security. The oversight bodies must closely oversee this collaboration.

Responsiveness and participation

- Intelligence oversight must ensure that governance and regulation of intelligence services are done in an inclusive and participatory manner, considering the impact that digital technologies may have on groups made vulnerable by discrimination.

- Intelligence services must always conduct themselves in a culture of service and duty to the nation, refraining from manipulation, intimidation, or censorship.

Human rights and gender equality

- Human rights and gender equality must be mainstreamed into the activities of both intelligence services and oversight bodies, at all levels.

- Training concepts for intelligence analysts and oversight actors must be developed which raise awareness of the propensity of AI-related systems to display significant gender and other biases and discrimination, and which offer an intersectional approach to eliminate discrimination.

WHAT TO READ NEXT

- Ryngaert, Cedric and van Eijk, Nico (2019)
  International Cooperation by (European) Security and Intelligence Services: Reviewing the Creation of a Joint Database in Light of Data Protection Guarantees
  International Data Privacy Law 9 (1) (April)

- Vieth, Kilian and Wetzling, Thorsten (2019)
  Data-driven Intelligence Oversight. Recommendations for a System Update
  Stiftung Neue Verantwortung (November)

- Katz, Brian (2020)
  The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection
  Washington, DC: Centre for Strategic and International Studies (CSIS)

- Born, Hans and Wills, Aidan (2012)
  Overseeing Intelligence Services: A Toolkit
  DCAF: Geneva

- Blanchard, Alexander and Taddeo, Mariarosaria (2023)
  The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations
  DISO 2, 12.

MORE DCAF SSR RESOURCES

DCAF publishes a wide variety of tools, handbooks and guidance on all aspects of SSR and good SSG, available free-for-download at **www.dcaf.ch**

Many resources are also available in languages other than English.

WHAT DCAF DOES

Help to improve the way national security sectors are governed.

Guide the development of sound, sustainable security governance policies.

Promote locally owned reforms that are inclusive, participatory, and gender responsive.

HOW WE DO IT

Provide technical expertise to nationally led SSG/R processes.

Build the capacity of state and non-state actors.

Publish research and knowledge products.

Promote internationally recommended good governance practices.

Advise on security sector-related legal and policy questions.

DCAF Geneva Centre for Security Sector Governance

DCAF – Geneva Centre for Security Sector Governance

Maison de la Paix
Chemin Eugène-Rigot 2E
CH-1202 Geneva
Switzerland

info@dcaf.ch
+41 22 730 94 00

www.dcaf.ch