DCAF 25 YEARS

SSR BACKGROUNDER

# ARTIFICIAL INTELLIGENCE (AI) AND THE DEFENCE SECTOR

## ABOUT THIS SSR BACKGROUNDER

This SSR Backgrounder provides an overview of the intersection between artificial intelligence (AI) and the defence sector. AI is deployed in many domains, including education, finance, transport, healthcare, and national security. The defence sector, as a critical component of the broader national security sector, encompasses military capabilities and operations aimed at safeguarding a nation's sovereignty and interests. While AI has the potential to increase the efficiency of defence activities, it poses several challenges related to human rights and the good governance of the defence sector. This SSR Backgrounder defines AI and explores its applications in the defence sector, examines the risks to good governance, and offers insights on strengthening oversight through robust monitoring, enhanced transparency, accountability measures, and stakeholder collaboration.

## THIS SSR BACKGROUNDER ANSWERS THE FOLLOWING QUESTIONS:

## 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**
Alexandru Lazar and Dawn Lui for authorship; Gabriela Manea, Franziska Klopfer, Teodora Fuior, Alexander Walsh, and Ken Isaac for their comments and revisions; Alec Crutchley for copy editing; Petra Gurtner for layout and design.

**Series Editor**
Gabriela Manea

**To cite this publication**
DCAF – Geneva Centre for Security Sector Governance. Artificial Intelligence (AI) and the Defence Sector.
SSR Backgrounder Series. Geneva:
DCAF, 2025.

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

☎ +41 22 730 94 00
✉ info@dcaf.ch
🐦 @DCAF_Geneva

www.dcaf.ch

## WHAT IS ARTIFICIAL INTELLIGENCE (AI)?

Artificial Intelligence (AI) is a general-purpose technology that has the potential to improve the welfare of people and to help respond to global challenges. As illustrated in Figure 2, AI can be defined as a *machine-based system* that infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

The term *machine-based system* often refers to a system that uses *algorithms,* software, and hardware to perform tasks such as processing data, making decisions or controlling other machines or processes. An *algorithm* is a set of step-by-step instructions or rules designed to perform a specific task or solve a particular problem. They can range from simple instructions to complex sequences of operations.

An 'AI system' is a comprehensive integration of AI models, agents, data, and infrastructure designed to perform specific tasks autonomously or semi-autonomously, often within a broader operational environment. In this instance, it is important to differentiate between an 'AI model' and an 'AI agent' as these two terms will be mentioned in different parts of this SSR Backgrounder. An 'AI model' represents a mathematical or statistical representation of patterns in data, trained to perform a specific task. It takes input, processes it using learned parameters, and produces an output (i.e. ChatGPT). An 'AI agent' interacts with an environment to achieve goals autonomously. It perceives, decides, and acts, often using AI models as components within a broader framework.

For example, an AI system might include anything from an automated chatbot to an advanced autonomous vehicle. These systems rely on *machine learning algorithms,* sensors, and processors to interpret data and make decisions in real time. Instead of being programmed to only perform a task, *machine learning systems* are trained on large amounts of data, allowing them to identify patterns, improve their performance over time, and adapt to new information without human intervention.

AI is evolving rapidly and is contributing to a wide array of economic and societal advancements. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages. AI is nowadays deployed in many sectors, ranging from education, finance, and transport to healthcare and national security. In terms of national security, AI's transformative potential in the defence sector has gained significant attention from policymakers, military strategists, and scholars alike. Nonetheless, alongside its potential benefits, AI is increasingly seen as a double-edged sword, creating conditions that can perpetuate social inequalities, erode human rights, undermine democracy and good governance, and cause harm. Such harm might be either tangible or intangible, including physical, psychological, societal, or environmental harm.

Governing AI is one of the biggest challenges faced by the international community. While the governance debate around AI regulation has moved from the question of ***whether*** it should be regulated to ***how*** it should be regulated, the exact governance framework remains open at the time of writing this SSR Backgrounder, as there is not yet a *universally accepted regulatory framework* for AI in the defence sector. Regulating AI in the military domain presents distinct challenges compared to civilian AI governance. For example, military AI applications often involve classified information and strategic assets, necessitating stringent security measures. The use of AI in autonomous weapons and military decision-making raises unique ethical concerns, such as the potential for unintended harm from AI-driven military actions. At the same time, due to the increasing levels of volatility in the global system, defence establishments worldwide are seeking to secure a strategic advantage in this domain, rendering the overarching task of regulating military AI systems even more complicated.

However, principles such as 'responsible AI' or 'human-centred AI' have gained momentum in the wider debate on AI and seem to provide a strong foundation for shaping future governance frameworks. Responsible AI refers to the ethical and accountable development, deployment, and use of AI systems. It encompasses principles, guidelines, and practices aimed at ensuring that AI technologies are designed and implemented in ways that prioritize fairness, transparency, accountability, privacy, and societal wellbeing. The human-centric approach to AI strives to ensure that human values are central to the way in which AI systems are developed, used, and monitored. It implies respect for fundamental rights, human dignity, and entails considerations of the natural environment and other living beings as part of the human ecosystem.

This SSR Backgrounder serves as an introduction to the application of AI within the defence sector. Its objective is to present the potential benefits and risks that AI systems introduce to the good governance of the defence sector, as well as to provide suggestions for robust oversight practices on the use of AI by defence actors more broadly.

To read more about technological developments in the security sector, please consult the Digitalization and SSG/R: Projections into the Future report, as well as the SSR Backgrounders on Digitalization and Security Sector Governance and Reform and Intelligence Oversight in the Age of Digitalization.

### FIGURE 1 CONCEPTUAL CLARIFICATIONS

**Artificial Intelligence (AI):** AI is the field that enables computers to perform tasks that typically require human intelligence, such as reasoning, learning, problem-solving, perception, and language understanding. It includes narrow AI (task-specific) and general AI (human-like intelligence).

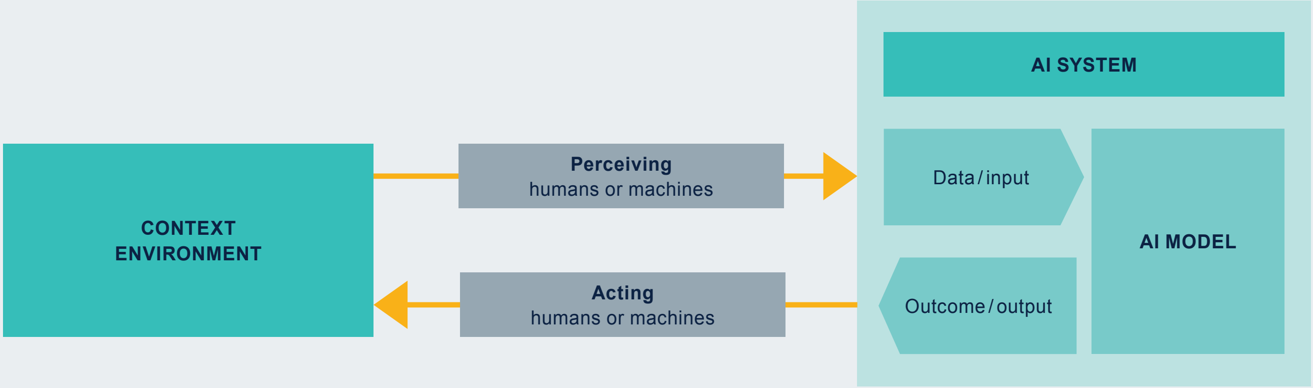
**Machine Learning (ML):** A subset of AI where computers learn from data to make predictions without explicit programming. ML includes supervised learning (labeled data), unsupervised learning (finding patterns), and reinforcement learning (learning through trial and error).

**Deep Learning and Neural Networks:** Deep Learning, a subset of ML, uses artificial neural networks (ANNs) with multiple layers to analyze complex data patterns. Neural networks, inspired by the human brain, process inputs through interconnected nodes to make predictions, powering applications like image recognition and natural language processing.

**Natural Language Processing (NLP):** NLP is a branch of AI that enables computers to understand, interpret, and generate human language. It is used in applications like chatbots, speech recognition, translation, and sentiment analysis. Large-scale language models, such as GPT (Generative Pre-trained Transformer), leverage deep learning techniques to enhance NLP capabilities.

**Large Language Models (LLMs) and Generative AI:** LLMs process vast text data to understand and generate human-like language. Generative AI (GenAI) goes further, creating original content—text, images, audio, or video—by learning patterns from large datasets.

### FIGURE 2 FUNCTIONING OF AN AI SYSTEM



Source: OECD.AI Policy Observatory

## WHAT IS THE DEFENCE SECTOR?

The defence sector is the domain of public administration responsible for military power. It is a part of the broader national security sector and comprises the armed forces, their executive controlling authorities, other state agencies permanently or occasionally involved in defence matters, commercial defence service providers, and civil society organizations involved in overseeing defence activities. For more information on the defence sector, please refer to the SSR Backgrounders on Defence Reform and Armed Forces.

The role of the defence sector is twofold:

1. **Operational conduct** (i.e. command and execution of military operations).

2. **Logistics, resource management, and oversight** (i.e. financial management, procurement of military equipment, recruitment, training and administration of personnel, as well as oversight of military operations).

FIGURE 3 **ACTORS IN THE DEFENCE SECTOR**

| ACTOR | ROLE |
|---|---|
| Armed forces | • Conduct military operations<br>• Implement strategies and tactics to defend the state from external threats and ensure national security<br>• Execute orders from executive controlling authorities |
| Executive controlling authorities | • E.g., the president or prime minister, the minister of defence, the national security council, military chiefs of staff, defence ministries, and other relevant government agencies<br>• Set overall defence policy and objectives<br>• Allocate resources for defence activities<br>• Make decisions on military strategies and deployments |
| Domestic security providers | • E.g., law enforcement agencies (such as police forces), intelligence services, border security, emergency services, and private security companies<br>• Cooperate with defence forces to gather and share information related to national security threats<br>• Provide information and insights to decision-makers to support defence policy and operations |
| Internal and external oversight committees | • E.g., parliamentary defence committees, governmental watchdogs, internal audit units, ombudsman offices, independent commissions, and international organizations<br>• Provide independent oversight and scrutiny of defence activities and expenditure<br>• Review adherence to laws, regulations, and ethical standards within the defence sector<br>• Identify inefficiencies, risks, and areas for improvement in defence operations |
| Commercial defence providers | • E.g., private military contractors, defence technology companies, arms manufacturers, cybersecurity firms, and logistics or infrastructure companies<br>• Develop and supply necessary material and technology<br>• Offer specialized services, such as logistics, intelligence, cybersecurity, and maintenance<br>• Provide flexible solutions and services for responding to emerging threats, crisis situations, or military engagements |
| Civil society organizations | • E.g., non-governmental organizations (NGOs), think tanks, advocacy groups, academic institutions, human rights organizations, and media outlets<br>• The media advocates for transparency, accountability, and ethical practices in national defence policies and operations<br>• Think tanks conduct research and foster informed citizen participation in national defence issues<br>• NGOs monitor and report on potential human rights violations |

**FIGURE 4 BENEFITS OF AI TO THE DEFENCE SECTOR**

| AUTOMATION OF ROUTINE TASKS | SITUATIONAL AWARENESS | COMMAND AND CONTROL |
|---|---|---|
| • AI can streamline administrative burdens by automating routine processes like financial tasks.<br>• AI can improve budget forecasting accuracy and efficiently detect anomalies in financial data.<br>• By automating these tasks, defence agencies can free up human resources for more complex, strategic initiatives. | • AI can analyse vast data sources, providing defence agencies with real-time insights into evolving threats.<br>• AI systems can quickly identify potential threats that could be missed by human operators.<br>• Improved situational awareness can minimize risks to defence personnel. | • AI can swiftly analyse vast data streams, offering commanders real-time information.<br>• This allows for agile, informed responses to threats and boosts operational efficiency.<br>• AI in command and control can strengthen defence forces' superiority and readiness in complex environments. |

## WHY IS AI USED BY THE DEFENCE SECTOR?

The defence sector is at the forefront of innovation and technology. Defence organizations are among the largest consumers and producers of data, as they already own disproportionately more information than others due to the nature of their work. Considering the amount of assets involved – including people, equipment, information, and technology – as well as the reality that defence departments are increasingly being asked to do more with smaller budgets, AI systems are perceived as attractive solutions. The defence sector's use of AI is mainly driven by its potential to provide a strategic advantage by transforming existing military capabilities. More precisely, AI technologies offer the promise of enhanced situational awareness and decision-making for executive authorities while minimizing the risks to defence personnel.

Below are a few examples of how AI is and can be used in the defence sector:

- **Warfare systems:** Integrated into autonomous weapons, drones, and smart munitions, to mention a few. For example, an AI agent can coordinate multiple drones to act collaboratively in reconnaissance, combat, or logistical support operations.
- **Cybersecurity:** Strengthen cyber defences by detecting, predicting, and countering cyber threats in military networks and infrastructure.
- **Simulation and training:** Provide realistic training environments for soldiers, improving readiness and tactical skills in various scenarios.

Figure 4 illustrates how AI-powered solutions can enhance situational awareness and planning, optimize resource allocation, and streamline operational processes for various defence actors, with the purpose of increasing the effectiveness and efficiency of defence organizations in safeguarding national security interests.

As a result, using AI in the defence sector provides the opportunity to remove extraneous, low-value activities that ultimately distract from the core mission, while assisting various actors to streamline and centralize bureaucratic processes. Nevertheless, the lack of transparency of many AI systems and the technology powering them raises major ethical concerns, especially if these systems control multimillion-dollar pieces of lethal military hardware.

## WHAT ARE THE RISKS AI POSES TO THE DEFENCE SECTOR?

**Biases and discrimination:** As AI systems are shaped by human design and data, they carry the risk of perpetuating existing societal biases, further exacerbating issues of discrimination and unfair targeting during military operations.

**Cybersecurity risks:** AI is transforming the cyber threat landscape by lowering the entry barriers for cybercriminals. The potential for AI to enhance social engineering tactics, such as phishing and deepfake technology, is becoming increasingly evident and poses a considerable challenge for the defence sector. Moreover, like many other digital tools, AI systems are prone to cyberattacks themselves. Common attacks include:

- **Prompt injection attacks,** where a malicious actor manipulates an AI system's prompt (input) to override its intended behaviour, bypass security measures, or extract sensitive information. This can manipulate military AI decision-making systems, leading to unauthorized actions, misinformation, or compromised classified intelligence.
- **Adversarial attacks,** where manipulated data is fed into AI systems to cause errors or misclassifications. Such misclassifications can lead to operational failures or friendly fire incidents for defence actors.
- **Model poisoning,** where malicious actors compromise the training data to corrupt the AI model. Such an attack could allow adversaries to manipulate outcomes, disrupt operations, or gain strategic advantages.
- **Data extraction attacks,** where sensitive information is leaked by exploiting the AI system's outputs. This can lead to the leak of classified intelligence, operational strategies, or defence infrastructure details, compromising national security and giving adversaries a tactical edge.

**Disinformation:** AI tools can be used to generate or spread disinformation, such as the creation of deepfake videos where military leaders make misleading statements, or the automated generation of fake news articles or social media posts that distort the narrative around military operations.

**Privacy:** AI surveillance tools in the defence sector may infringe on the privacy rights of individuals by collecting and analysing large volumes of personal data without adequate safeguards.

**FIGURE 5 APPLICATIONS OF AI IN THE DEFENCE SECTOR**

| ACTOR | DETECTION | PLANNING | OPERATIONS | LOGISTICS |
|---|---|---|---|---|
| **Armed forces** | Collect and analyse relevant data from various sources to identify enemy movements, threats and anomalies | Assist in strategic and tactical planning by analysing vast datasets, predicting future scenarios, and optimizing resource allocation | Support real-time military engagements; provide commanders with actionable intelligence | Automate administrative tasks such as logistics, supply chain management, and personnel scheduling |
| **Executive controlling authorities** | Assist executives in drafting legislation and security policies | Analyse risks and evaluate alternative courses of action for defence capabilities and readiness | Provide real-time insights into operational effectiveness, enabling them to adjust resources in response to changing needs | Automate administrative tasks such as budget planning, contract management, and asset tracking; improve efficiency and accountability in defence procurement and logistics operations |
| **Domestic security providers** | Process and analyse large volumes of domestic security data to identify patterns, trends, and potential threats | Identify high-value targets, prioritization of threats, and development of strategic reports | AI-powered surveillance and reconnaissance systems enable enhanced precision | Automate data processing, report generation, and information dissemination; streamline workflows |
| **Internal and external oversight committees** | Monitor and analyse defence expenditure, procurement processes, and compliance with regulations to detect fraud, waste, or abuse within defence organizations | Support oversight activities by analysing defence policies, evaluating strategic plans, and assessing the effectiveness of defence programs and initiatives | Provide real-time insights into defence operations, budget execution, and performance metrics; facilitate accountability and transparency | Automate audit procedures, risk assessments, and compliance checks; improve the efficiency and effectiveness of oversight functions; and ensure adherence to legal and regulatory requirements |
| **Commercial defence providers** | Develop AI tools to detect and prevent cyber threats | Support strategic planning and risk assessment; automate forecasting tools to optimize resource allocation | Develop and deploy AI-powered drones for surveillance | Streamline maintenance and equipment readiness through predictive AI; use AI algorithms to optimize supply chain management |
| **Civil society organizations** | Identify and report on potential human rights violations | Advocate for transparent and ethical AI use in defence | Support community engagement and awareness initiatives regarding AI-powered defence systems | Promote accountability in defence spending and resource use to develop or acquire AI tools |

## HOW DOES AI IMPACT GOOD GOVERNANCE OF THE DEFENCE SECTOR?

In addition to these risks, the use of AI by the defence sector presents further challenges to the implementation of good security sector governance, in particular:

- **Accountability:** The opacity of AI technology and decision-making algorithms can hinder the ability to trace and understand how decisions are made, especially when it comes to target-setting or lethal action decisions. As a result, it could become challenging to hold individuals or institutions accountable for errors, biases, or misuse of AI systems.

- **Transparency:** Lack of transparency in AI systems can lead to uncertainty and distrust among citizens. In turn, this would lead to undermining confidence in defence institutions with a two-fold impact, both on ongoing military operations and domestic support.

- **Rule of law:** AI systems may inadvertently violate legal and ethical principles, such as international humanitarian law, due to biases in algorithms and design, errors in decision-making, or lack of human oversight. Undermining the rule of law and adherence to established legal frameworks can have severe consequences for both individuals and states.

- **Participation:** Limited transparency and understanding of AI technology can hinder meaningful participation and engagement of stakeholders, including defence personnel, civil society organizations, and marginalised communities.

- **Responsiveness:** Overreliance on AI systems may diminish human judgment and intuition, which is essential for timely and responsive decision-making in rapidly evolving situations. This can potentially delay or hinder effective responses to emerging threats or crises.

- **Effectiveness:** Biases in AI systems may lead to discriminatory practices, diminishing the effectiveness of defence operations and resource allocation, and undermining the achievement of strategic objectives.

- **Efficiency:** Lack of transparency, accountability, and oversight in AI systems can result in inefficiencies, such as errors in decision-making, duplication of effort, or misuse of resources, compromising the efficiency of defence operations and resource management.

Two further cross-cutting issues to consider are:

- **Human rights:** Lack of regulation, oversight, and accountability of AI systems can lead to violations of human rights, such as privacy infringements, surveillance abuses, discrimination, and targeting of vulnerable populations, undermining fundamental rights and freedoms protected by international law.

- **Gender equality:** AI systems may perpetuate gender biases present in training data, leading to discriminatory outcomes in recruitment, promotion, and decision-making processes within the defence sector. This can reinforce gender inequalities and hinder the advancement of women in military and defence-related professions.

To learn more about gender equality and human rights in the context of security sector governance and reform, please consult the DCAF SSR Backgrounders on Gender Equality and Good Security Sector Governance, Gender Equality and Security Sector Reform, and Human Rights and SSG/R.

### FEATURES OF GOOD SSG

When the principles of good governance are applied to the defence sector, the state provides security for the population effectively and accountably within a framework of democratic, civilian control, rule of law and respect for human rights. Good security sector governance (SSG) is a collection of principles, not an institutional model, and therefore the same core principles apply differently in the context of each national defence sector. Establishing good SSG is a matter of constant ongoing adjustment as security threats and needs change. No defence sector is beyond the need for improvement. Although each defence sector will face distinct threats and needs, there are some typical institutional features of good SSG.

## HOW CAN THE DEFENCE SECTOR STRENGTHEN OVERSIGHT OF THEIR USE OF AI?

Defence organizations can mitigate risks and maximize the benefits of AI technologies while upholding ethical standards and compliance with legal and regulatory frameworks. These organizations could implement robust monitoring mechanisms, enhance transparency and accountability, and foster collaboration among internal oversight bodies, external stakeholders, as well as their international counterparts.

Figure 6 below outlines how different defence sector actors can strengthen oversight of their use of AI.

**FIGURE 6 OVERSIGHT OF AI APPLICATIONS IN THE DEFENCE SECTOR**

| ACTOR | DOMESTIC REGULATORY FRAMEWORK | TRANSPARENCY AND ACCOUNTABILITY | PARTNERSHIPS & COLLABORATION |
|---|---|---|---|
| **Armed forces** | Implement AI-specific audit and review processes to monitor the development, deployment, and performance of AI systems | Enhance transparency in AI systems by disclosing unclassified information about data sources, algorithms, and decision-making processes to stakeholders, including defence personnel and external oversight bodies | Collaborate with civil society organizations, academic institutions, research organizations, and industry partners to exchange best practices, share lessons learned, and foster innovation in AI governance and oversight |
| **Executive controlling authorities** | Establish dedicated oversight bodies or committees to implement risk management frameworks to identify, assess, and mitigate potential risks associated with AI adoption, including ethical, legal, and security considerations | Publish AI impact assessments and reports detailing the deployment, performance, and outcomes of AI systems in defence operations | Strengthen collaboration with parliamentary committees, government watchdogs, and independent auditors to provide regular updates and reports on AI initiatives and investments in defence |
| **Domestic security providers** | Establish independent review panels to monitor and evaluate the ethical and legal implications of AI use in domestic security activities | Implement internal controls and audits to ensure compliance with legal and ethical guidelines governing AI use in domestic security | Foster partnerships with human rights organizations, privacy advocates, and academic experts to conduct independent assessments and reviews of AI systems used in domestic security activities; Promote transparency and accountability in AI governance |
| **Internal and external oversight committees** | Implement whistleblower protection mechanisms to encourage reporting of AI-related concerns or misconduct within defence organizations | Develop open-source platforms for citizens to submit any issues or abuses committed by defence actors when using AI technology | Continuous engagement between internal and external stakeholders, including civil society groups and industry experts, to solicit feedback and recommendations for enhancing AI oversight mechanisms |
| **Commercial defence providers** | Regularly test, evaluate, and update AI models to adhere to the latest regulations and ethical standards | Ensure transparency in AI algorithms and decision-making processes; establish clear internal accountability structures for AI development and commercialisation | Collaborate with government, civil society, and tech companies to enhance AI ethics |
| **Civil society organizations** | Independent monitoring and auditing of AI-driven defence activities and outcomes | Advocate for public disclosure of AI use and impact in defence; promote accountability through public reporting and watchdog roles | Engage with defence entities to ensure ethical AI practices; work with international organizations on AI regulation in defence |

## WHAT TO READ NEXT

- Centre for Humanitarian Dialogue
  **Code of Conduct on Artificial Intelligence in Military Systems**
  Geneva: HD 2021

- Cheong, Sandra
  **Intelligence Oversight in the Age of Digitalization**
  Geneva: DCAF 2024

- Davison, Neil
  **A legal perspective: Autonomous weapon systems under international humanitarian law**
  Geneva: ICRC 2016

- Deloitte
  **The Age of With™ – The AI advantage in defence and security**
  Ontario: Deloitte: 2024

- European Parliament and Council of the European Union
  **EU Artificial Intelligence Act**
  Brussels: EU, 2024

- Evans, Thamy
  **Defence Reform**
  Geneva: DCAF 2019

- Herd, Graeme P., Puhl, Detfel, and Costigan, Sean
  **Emerging Security Challenges: Framing the Policy Context**
  Geneva: GCSP, 2013

- Huhtanen, Heather and Triquet, Veerle
  **Gender Equality and Good Security Sector Governance**
  Geneva: DCAF 2015

- ISSAT Advisory Note
  **Artificial Intelligence and SSG/R**
  Geneva: DCAF 2023

- Lui, Dawn and Lazar, Alexandru
  **Digitalization and SSG/R: Projections into the Future**
  Geneva: DCAF 2023

- Lui, Dawn
  **Digitalization and Security Sector Governance and Reform**
  Geneva: DCAF 2022

- OECD.AI Policy Observatory
  **Resources on AI**
  Paris: OECD 2024

- Stanford University
  **The AI Index Report: Measuring trends in AI**
  Stanford: Stanford University, 2024

- Triquet, Veerle and Watson, Callum
  **Gender Equality and Security Sector Reform**
  Geneva: DCAF 2015

- Ulnicane, Inga
  **Intersectionality in Artificial Intelligence: Framing Concerns and Recommendations for Action**
  Warwick: Social Inclusion, vol. 12, 7543

- US Department of State
  **Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy**
  2024

### 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 25 YEARS

**DCAF – Geneva Centre for Security Sector Governance**

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

☎ **+41 22 730 94 00**
✉ **info@dcaf.ch**
🐦 **@DCAF_Geneva**

**www.dcaf.ch**