Kingdom of the Netherlands

DCAF 25 YEARS

Comprehensive Toolkit for Defence Ethics

FROM PRINCIPLES TO PRACTICE

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's Foundation Council members represent over 40 countries and the Canton of Geneva. Active in over 60 countries, DCAF is internationally recognized as one of the world's leading centres of excellence for security sector governance (SSG) and security sector reform (SSR). DCAF is guided by the principles of neutrality, impartiality, local ownership, inclusive participation, and gender equality. For more information, visit www.dcaf.ch and follow us on social media.

Acknowledgements

This work is part of DCAF's Enhancing SSG/R Policy & Practice programme (P&P), which forms part of DCAF's strategic partnership with the Netherlands' Ministry of Foreign Affairs Department of Stabilisation and Humanitarian Aid (NL MFA DSH). The authors gratefully acknowledge the support of the Netherlands and express sincere thanks to Evgenia Dorokhova, whose support has been essential for the successful implementation of this project. We also extend our appreciation to Darko Stančić, Head of Europe Asia Entity, whose strategic support and encouragement have been instrumental in shaping this toolkit. We are indebted to the reviewers Viorel Cibotaru, Leonid Polyakov, Anna Dolidze, Robert Hranj, Andrzej Fałkowski, Philippe Boutinaud, Abigail Robinson, and Paulo Costa, whose sharp, insightful, and constructive feedback have significantly strengthened the quality and added value of this publication. Special thanks are owed to Professor George Lucas and Professor David Whetham, whose foundational ideas and long-standing work in defence ethics are reflected across multiple sections of this toolkit. We also extend heartfelt appreciation to colleagues from the Ministry of Defence of Ukraine, Building Integrity Training and Educational Centre (BITEC) of the National Defence University of Ukraine, the Ministry of Defence of Tunisia, Ministry of Defence of Georgia, and defence counterparts in Kyrgyzstan, whose engagement during pilot training programmes provided indispensable insights and real-world perspectives. We further acknowledge the contributions of the Business and Security Entity of DCAF and the DCAF team in Tunisia.

Published in Switzerland by DCAF – Geneva Centre for Security Sector Governance.

Authors: Dr. Grazvydas Jasutis and Rebecca Mikova

Copy editor: Dianne Battersby

Research contributors: Vlasta Kovbasa and Anais Fiault

Layout and design: Nadia Joubert

Reviewers: Dr. Viorel Cibotaru, Former Minister of Defence of Moldova; Leonid Polyakov, Former Deputy Minister of Defence of Ukraine; Dr. Anna Dolidze, Former Deputy Minister of Defence of Georgia; Rear Admiral Robert Hranj, Former Chief of General Staff of Croatia; Dr. Andrzej Fałkowski, Lt General (Ret.) of the Polish Armed Forces; Gen. Philippe Boutinaud, Senior Security and Strategy Adviser at DCAF; Abigail Robinson, Former Defense Governance Adviser, U.S. Department of Defense; Paulo Costa, Senior Integrity Expert at DCAF

The authors have drawn on materials from defence ethics training programmes conducted in Georgia (developed by Prof. George Lucas and Prof. David Whetham), as well as from training experiences in Kyrgyzstan, Tunisia, and Ukraine.

Cover photo: Illustration by Nadia Joubert

ISBN: 978-92-9222-805-7

DCAF – Geneva Centre for Security Sector Governance

+41 22 730 94 00

info@dcaf.ch

www.dcaf.ch

© DCAF 2025. All rights reserved.

Table of contents

List of abbreviations 2
Executive summary 3
Introductory remarks to the Defence Ethics Toolkit 4
Introduction 5
Training delivery framework 8
Adult learning 12
Facilitators' techniques and tips 16

MODULE 1
Ethics, law and culture in the defence sector 20

MODULE 2
Ethics and leadership in the defence sector 30

MODULE 3
Key ethical dilemmas in the defence sector 40

3.1. Mistreatment and discrimination 41
3.2. Nepotism in the defence sector 51
3.3. Misuse of command authority and unprofessional behaviour 58
3.4. Gifts and bribes 64
3.5. Conflict of interest in the defence sector 70
3.6. Truth versus loyalty: Whistle-blowing 78
3.7. Ethical dilemmas during combat operations 84
3.8. Emerging technologies and cybersecurity in the defence sector 93

MODULE 4
Ethical decision-making in the defence sector 112

Concluding remarks 120
Further reading 121
Annex I 123
Annex II 125

List of abbreviations

AI	Artificial intelligence
BITEC	Building Integrity Training and Educational Centre (National Defence University of Ukraine)
COI	Conflict of interest
COMEDEF	Defence Ethics Committee (France)
DAG	Dyck Advisory Group
DAIC	Defence Artificial Intelligence Centre (UK)
DND	Department of National Defence (Canada)
DoD	Department of Defense (US)
DSS	Decision-support systems
ICRC	International Committee of the Red Cross
IHL	International humanitarian law
ISR	Intelligence, surveillance, and reconnaissance
LAWS	Lethal autonomous weapon systems
LOAC	Law of armed conflict
MoD	Ministry of Defence
NCO	Non-commissioned officer
PMSC	Private military and security companies
POW	Prisoner of war
PPE	Personal protective equipment
RAI	Responsible artificial intelligence
SSG	Security sector governance
SSR	Security sector reform
TEV&V	Testing, evaluation, verification & validation

Executive summary

This toolkit provides a practical and adaptable framework designed to strengthen ethical decision-making, integrity, and professionalism in the defence and security sector. Its primary aim is to equip military and civilian personnel with concrete tools, scenarios, and learning methods that help translate ethical principles into daily practice both in peacetime and during operations. The toolkit supports institutions in building resilient organizational cultures grounded in accountability, transparency, and respect for the rule of law.

The publication is structured to guide users from foundational concepts to applied practice. It begins with detailed guidance for trainers and explains the core principles of ethics. This is followed by information on ethical leadership, consequences of abuse of authority, ethical dilemmas, nepotism, conflict of interest, and other topics paramount to the defence sector and its resilience. The sections present real-world case studies (which have been anonymized), ready-to-use training tasks, and discussion prompts, enabling instructors to integrate the toolkit into existing training programmes with minimal adaptation.

The intended audience includes military instructors, professional military education institutions, defence sector managers, integrity officers, and civilian oversight bodies. It is relevant for international partners engaged in capacity building, as well as for operational commanders seeking practical resources to support ethical leadership within their units.

The toolkit has been externally and internally vetted to ensure methodological relevance to diverse defence environments, and it has been piloted and tested in multiple contexts, including field-level and institutional settings in Kyrgyzstan, Tunisia, and Ukraine. Feedback from these pilots has informed the refinement of exercises, improved cultural adaptability, and ensured that the toolkit responds to real operational and organizational challenges.

A short illustrative video 'Understanding and responding to unethical behaviour in Ukraine' from the training session in Yaremche, Ukraine demonstrates how the toolkit functions in practice, highlighting group exercises, role-playing techniques, and the implementation of multisensory learning methods: https://www.youtube.com/watch?v=9RaNtOkdqTc.

Overall, this toolkit offers a comprehensive field-tested resource that strengthens ethical culture, enhances decision-making under pressure, and supports the long-term professionalism of defence institutions.

Introductory remarks to the Defence Ethics Toolkit

George Lucas
Distinguished Chair of Ethics, emeritus
U.S. Naval Academy (Annapolis, Maryland, US)

This seems hardly the most propitious moment in international relations for addressing 'defence ethics'. Nations currently engaged in armed conflict with one another instead seem bent on ignoring the most basic legal principles and moral scruples when resorting to military force to resolve their differences, particularly through the disproportionate use of deadly force and the deliberate targeting of one another's civilian non-combatants and civilian objects (infrastructure) – behaviours explicitly prohibited in international humanitarian law.

Yet, as the myriad case studies of unethical and illegal behaviour by military forces and defence organizations in this 'defence ethics toolkit' illustrate, such rampant and widespread unethical behaviour serves only to undermine rather than further the goals of public defence and national security. Indeed, by showing the counterproductive and destructive effects of ignoring ethics in national defence, the authors of this toolkit provide decisive evidence for the continuing relevance of ethics in the best and most effective practices of national defence policy generally. The NATO member nations, together with the candidates seeking membership in NATO, are, in particular, committed to the adoption and furtherance of ethical practices in military affairs, and to reaping the benefits of such practices in providing safety and security for the citizens they have committed to serve and protect.

This ethics toolkit itself serves to renew and strengthen each country's commitment to institutional trustworthiness and financial integrity in providing for their respective citizens' safety and political security, as well as to examine and improve each country's military forces in practices ranging from the recruitment and training of military personnel to authorizing the procurement of new defence weapons systems. Under the watchwords 'transparency, integrity, and accountability', nations through the use of this toolkit share best practices, identify areas of deficient performance, and study new and emerging threats to their effective operation in the military conflicts and challenges of the new millennium.

Introduction

This introduction section has been adapted from a training manual on police integrity published by DCAF in 2015.[1]

The present toolkit has been developed to provide practical guidance for trainers and facilitators, so they are able to deliver training on defence ethics to both military and civilian personnel in the defence sector. The toolkit will equip the defence sector with content and methodologies to address various ethical dilemmas and will guide responsible decision-makers in navigating these challenges and responding appropriately to specific situations.

The methodology, content, and approach outlined in this manual have been reviewed by experts from DCAF as well as by external specialists from diverse countries and professional backgrounds. As such, the toolkit is designed to be adaptable for use in any country, with appropriate modifications to suit local contexts.

We recommend adopting a 'train-the-trainers' approach to maximize the impact of this manual. The following steps should be considered:

Select facilitators with the appropriate profile and competencies for defence ethics training.

Organize a facilitation course to prepare and equip the selected staff.

Conduct and review a pilot course delivered by the newly trained facilitators.

Consolidate and adapt the training manual and methodology to facilitate further implementation of defence ethics training across security and defence personnel.

1 Paulo Costa and Isaline Thorens, *Training Manual on Police Integrity* (Geneva: DCAF, 20 December 2015), https://www.dcaf.ch/node/12922

Selecting facilitators

Defence ethics training requires a specific approach in terms of content and delivery methodology. To ensure the effectiveness of training outcomes, we recommend that you adhere to the following criteria when selecting facilitators:

- **Willingness:** Individuals must be motivated and open to become facilitators on defence ethics.
- **Role model:** Facilitators should demonstrate a strong reputation, be respected and well regarded by their peers, and serve as a positive example through their conduct.
- **Communication skills:** Facilitators must possess excellent verbal and non-verbal communication skills and be comfortable with public speaking.
- **Work experience:** Facilitators should have a minimum of two years' operational experience within the security and defence sector.

Definitions for the roles of 'trainer' and 'facilitator'

It is crucial to distinguish between the roles of 'trainer' and 'facilitator'. These terms are often used interchangeably but have important underlying differences. While a trainer assumes an active role in educating and in transmitting knowledge, a facilitator guides a group in understanding their shared objectives and supports them in planning how to achieve these goals. In this sense, a facilitator undertakes a 'neutral' role, refraining from taking a specific position in the course of discussions.

The facilitator's role is to enhance the discussion creatively rather than simply lead it. They should have the ability to understand and navigate group dynamics effectively – recognizing who is dominating the conversation and finding ways to balance participation, noticing who is withdrawn and needs encouragement to contribute, and being aware of anyone who appears disengaged and how to draw them into the learning process.

Organizing a facilitation course

The course provided for the facilitators should be tailored to the number of participants and their prior experience in training or facilitation. In all cases, it is recommended that the minimum duration for a facilitation course is five consecutive days.

Delivery and review of a pilot course

Upon successful completion of the facilitation course, and prior to delivering training to all staff in the organization, it is recommended that the trained facilitators conduct at least one pilot course to their peers. This pilot session will serve as an opportunity for both facilitators and organizers to review, evaluate, and adjust the course's content and methodology in preparation for full-scale implementation. Both elements – content and methodology – should be carefully assessed by the facilitators and the training organizers.

The pilot course should ideally be conducted shortly after the facilitation course, preferably during the following week and not later than one week afterwards. This timing helps ensure that the knowledge and skills acquired during the facilitation course are fully retained and effectively applied, as longer delays between the two phases may diminish the training's overall effectiveness.

Consolidating and adapting the manual and methodology

A formal revision process should follow the delivery of the pilot course, bringing together both the facilitators and training organizers. Together, they should assess the outcomes of the pilot session and adjust the content and methodology to better align with the specific needs of the organization. It should be noted, however, that training is an ongoing process – one that requires continuous review, evaluation, and adaptation to evolving circumstances.

Multisensory learning and teaching

Multisensory learning is a teaching approach that engages multiple senses at the same time. This can include sight, sound, touch, taste, smell, and movement.[2] When learners engage multiple senses, their ability to understand and retain information increases significantly. This occurs because the material is processed through several neural pathways, creating stronger cognitive associations and reinforcing memory. For these reasons, trainers should deliberately design tasks that activate more than one sensory channel – such as visual, auditory, and tactile modes – to enhance comprehension, engagement, and long-term retention. Finally, the application of multisensory learning creates a more diverse and engaging teaching environment.

2 See https://orbrom.com/multisensory-learning-students-special-needs

Training delivery framework

This section has been adapted from a training manual on police integrity published by DCAF in 2015.[3]

Module structure

The proposed structure for the in-service training for defence and security personnel encompasses the following topics (modules):

1. Ethics, law and culture in the defence sector
2. Ethics and leadership in the defence sector
3. Key ethical dilemmas in the defence sector
   - **3.1.** Mistreatment and discrimination
   - **3.2.** Nepotism in the defence sector
   - **3.3.** Misuse of command authority and unprofessional behaviour
   - **3.4.** Gifts and bribes
   - **3.5.** Conflict of interest in the defence sector
   - **3.6.** Truth vs loyalty: Whistle-blowing
   - **3.7.** Ethical dilemmas during combat operations
   - **3.8.** Emerging technologies and cybersecurity in the defence sector
4. Ethical decision-making in the defence sector

The modules can be delivered either as a complete sequence or selected based on a needs assessment of the specific organization or target audience. If covering all topics in a single workshop is not feasible, this toolkit can serve as a resource from which modules can be chosen according to priority. Activities and methodological support can be modified, excluded, or enhanced, depending on the context and timeline.

We recommend delivering 3 to 5 modules per day, with each module lasting between 45 minutes and 1.5 hours. Furthermore, in order to maintain the attention span of the participants, regular breaks should be scheduled. Providing coffee/tea and light refreshments during these breaks helps participants to remain energized and fosters an informal atmosphere that encourages continued discussion and the exchange of personal experiences.

3 Paulo Costa and Isaline Thorens, *Training Manual on Police Integrity* (Geneva: DCAF, 20 December 2015), https://www.dcaf.ch/node/12922

Course introduction

Before beginning the first module, providing an introduction to the course or workshop is recommended. Key elements to cover include:

- **Facilitator introduction:** Introduce yourself, sharing your background and role. Clarify that the course is not intended to teach but rather to facilitate discussion and build on participants' professional experience.
- **Participant introduction:** Invite participants to briefly introduce themselves, including their role and relevant experience, to break the ice and contextualise discussions.
- **Context:** Outline the purpose of the training and why participants are engaging in a defence ethics course.
- **Agenda:** Explain the agenda, the sequence of modules, and the links between the different modules you will be covering. Distribute copies of the agenda to the participants at the beginning of the workshop.

Supporting materials

Handouts

Handouts are intended to be distributed to participants ahead of the activities.

Methodological support

The toolkit includes support materials (tasks and exercises) that are designed to help you facilitate specific activities and guide discussion towards key points.

Further reading

The list of further reading materials contains publications that will be useful for those who are not sufficiently familiar with the topics covered in the modules or who simply want to deepen their understanding of a certain topic to feel more confident in facilitating discussions.

Effective use of learning aids

Learning or visual aids play a crucial role in effective training facilitation. Various types of learning aids are available, and the choice of which to use should be guided by the learning objectives, participants' learning styles, and the overall training strategy. This toolkit encourages the use of flip charts, PowerPoint presentations, videos, and participant handouts to support different training activities.

- **Flip charts** are particularly effective for brainstorming exercises. They are commonly used for developing concepts, outlining ideas, and recording participants' comments during group discussions.
- **Videos** are valuable tools for generating discussion on particular topics. Participants can react to the ideas presented and reflect on them through the lens of their own experiences. However, if a video is in a language other than the participants' first language, it is essential to provide accurate subtitles or simultaneous interpretation to ensure full understanding and engagement.
- **PowerPoint** presentations can be a powerful way to visualize key points and structure information. However, they are often overused or used in a counterproductive way. The most important factor to remember is that PowerPoints should support – not replace – the facilitator. They are meant to guide the session and not serve as a script for a reading exercise. When using PowerPoints, ensure that participants remain engaged by encouraging discussion and interaction rather than passive listening.

Always run a test prior to starting the workshop: Check that all multimedia tools are functioning properly, ensure the screen is clearly visible from all angles of the room, and review the handouts for accuracy and completeness. Furthermore, it is advisable to always have a backup plan in case of any unexpected issues. Prepare more handouts than the number of participants and have alternative learning aids ready to ensure the session can continue smoothly.

Participants

The training is intended for personnel in the defence and security sector, encompassing both military and civilian roles. Based on experience, these modules are most effective when facilitated in small groups, ideally with no more than 15 participants. Groups should be gender-balanced and may include participants of different specialisations and ranks.

Facilitators

It is recommended that modules be prepared and delivered by teams of two to three facilitators. This allows one facilitator to assume the leading role and focus fully on engaging with participants, while the other facilitators provide support, such as collecting ideas during brainstorming activities, distributing handouts, taking notes, and assisting with activities. Additionally, alternating voices and facilitation styles can enhance the dynamics of the course and maintain the attention of the participants. Wherever possible, teams of facilitators should be gender-balanced.

Creating a favourable learning environment

It is the facilitator's responsibility to ensure that both the physical and psychological aspects of the learning environment are conducive for effective participation. From a physical perspective, recommended seating arrangements include either a 'U-shape' or a 'Café style' (small round tables with four to five participants each). The U-shape is particularly effective when facilitation involves presentations with flipcharts and projectors, while still supporting activities in pairs or threes. The Café style fosters collaboration and peer-to-peer learning in a more informal setting and makes it easy to rotate participants between activities. The psychological aspect focuses on the creation of a safe and supportive atmosphere in which participants feel comfortable to freely voice their concerns and share experiences, trusting that their contributions will remain confidential. Furthermore, if training sessions are provided in a language other than the participants' first language, simultaneous interpretation should be provided in order to facilitate understanding and discussion.

Course evaluation

To gauge how well the course has been received, we recommend distributing a brief evaluation form at the conclusion of all activities. The feedback will enable facilitators to identify areas for improvement and adjust their approach in future sessions. Furthermore, this evaluation will be crucial for understanding if the objectives of the training have been met. If they have not, appropriate adjustments should be made to improve the content, delivery, or methodology.

Questionnaires are a common tool for evaluating training courses, and time should be allocated within the seminar agenda for participants to complete them. Return rates tend to drop if forms are taken home after the training. Alternatively, holding evaluation discussions with a sample of participants can yield more qualitative, reflective feedback. Post-training evaluation typically addresses the amount and level of content, delivery methods (timing, pace, participation), quality of feedback provided, and logistical aspects such as venue, accommodation, and catering.[4] In addition, evaluating what participants have learned and retained from the training is essential, and the Kahoot platform is recommended for this purpose.

4 DCAF – Geneva Centre for Security Sector Governance, *Toolkit on Police Integrity* (Geneva: DCAF, 2012), https://www.dcaf.ch/toolkit-police-integrity

Adult learning

> This section has been adapted from a training manual on police integrity published by DCAF in 2015.[5]

Adult learning refers to a range of formal and informal learning activities, both general and vocational, undertaken by adults after leaving initial education and training.[6]

While the substantive part of training – the content and messages delivered – is important, the right approach and strategy are key in ensuring effective adult learning outcomes. In the context of this toolkit, ethics relates more to values, attitudes, and beliefs than to knowledge alone. It is easier to develop knowledge or skills during training than it is to change values, behaviours, and attitudes, which lie at the core of a person's integrity; therefore, training methodologies must be selected with particular care. Approaches such as real-life scenarios, ethical dilemmas, gamification, and role plays are especially effective, as they promote reflection and move away from traditional lecturing.

The 'Hole in the Wall' experiment

In early 1999, Indian computer scientist and educational theorist Sugata Mitra conducted an experiment to test whether children could master something entirely new through self-directed learning. He installed a computer in a wall in a deprived area near New Delhi. No instructions, no teaching, no manual – just a computer with a multitude of applications freely accessible to anyone passing by. The results were remarkable: children from the surrounding community, many with no prior exposure to technology, quickly gathered around the device. With no preliminary knowledge or guidance – just through collective learning and peer-to-peer collaboration – they were able to explore its features and eventually started surfing the web. This experiment revealed that children have an innate capacity to learn, suggesting they are often more adaptable than adults when encountering new knowledge. This approach to instruction became known as minimally invasive education (MIE), a method that challenges the traditional top-down model of education.[7]

5 Paulo Costa and Isaline Thorens, *Training Manual on Police Integrity* (Geneva: DCAF, 20 December 2015), https://www.dcaf.ch/node/12922

6 European Commission, Directorate-General for Education, Youth, Sport and Culture, 'Adult Learning Initiatives', *European Education Area*, last modified 3 June 2024, https://education.ec.europa.eu/education-levels/adult-learning/about-adult-learning

7 Sugata Mitra, 'The Hole in the Wall Project and the Power of Self-Organized Learning', *Edutopia* (George Lucas Educational Foundation, 3 February 2012), https://www.edutopia.org/blog/self-organized-learning-sugata-mitra. This experiment, along with the principles of andragogy, was presented and discussed by BITEC trainers at DCAF's workshop on 'Understanding and Responding to Unethical Behaviour', held in Yaremche, Ukraine, in August 2025.

The principles of andragogy

Building on the aforementioned experiment, researchers concluded that children have an innate predisposition to learn. Adults, by contrast, are typically motivated by specific goals, practical needs, and an understanding of the value of learning. Recognizing this distinction, Malcolm Knowles developed the theory of andragogy (a term initially coined by German teacher Alexander Kapp) – the study of adult learning – as distinct from pedagogy, the practice of teaching children. Andragogy rests on the following six principles:

01 **The need to know.** Adults need to recognize the value, relevance, and purpose of what they are learning. To this end, at the beginning and throughout the training, facilitators should clearly communicate the reasons and objectives of the training.

02 **Self-direction.** Adults are self-directed and autonomous; thus, they expect to play an active role in influencing and shaping the learning process. Facilitators should involve and engage participants early in the process to achieve better results.

03 **The role of experience.** Previous experience serves as a critical resource for learning, and adults need to share that experience with others and be acknowledged for their experience. Facilitators should design activities with the aim of allowing participants to progress successfully as well as challenging participants to reflect on past errors, which provides a better foundation for future learning. Furthermore, while the expertise which the facilitators bring is important, they should respect the knowledge and experience of the participants.

04 **Relevance.** Adults are motivated to learn when they perceive the material as directly applicable to their professional responsibilities. Facilitators should constantly emphasize that ethics and integrity are relevant in both public and private spheres and choose topics that have immediate relevance for participants' professional lives.

05 **Problem-centred orientation.** Adults prefer to adapt a practical problem-solving approach that enables them to find solutions to real-life problems. Facilitators should provide participants with an opportunity to solve real problems in the training process.

06 **Internal motivation.** Adults seek to grow professionally, and they are primarily driven by internal rather than external motivation. While external motivators, such as promotion or an increase in salary, are sometimes effective, adults are primarily motivated by internal factors, such as self-esteem, boost of confidence, or self-actualization.

The principles of andragogy are particularly relevant for military leadership education, as they foster a growth-oriented mindset, facilitating the development of autonomous and adaptable leaders with higher-order cognitive skills. Understanding these principles and adopting a facilitative rather than an instructive role makes the learning participant-centred rather than trainer-centred. This fosters a so-called 'guide on the side' model in place of the traditional 'sage on the stage' approach.[8]

8 Tom H Skoglund, Patrick Risan, and Rino B Johansen, 'Andragogy in a Military Leadership Course', *European Journal of Education Studies*, Vol. 12: No. 3 (2025), https://doi.org/10.46827/ejes.v12i3.5866

Training cycle

The training cycle is an essential component of any training strategy, as learning is a continuous process. Thus, facilitators and any other stakeholders need to be involved in the process and have a clear understanding of the various stages of the training cycle to achieve satisfactory results.

For the purposes of this toolkit, the training cycle in Fig. 1 is applied:

Figure 1. Training cycle, adapted from R. Buckley and J. Caple (1995), quoted in A. Costa and M. Thorens, Training Manual on Police Integrity

The **needs assessment** stage is the starting point of any training strategy. Its primary objective is to identify the gap between the current level of performance and the desired level of performance. This assessment can be conducted at multiple levels: individual (evaluating the strengths and weaknesses of individuals); departmental or organizational (assessing whether existing training programmes are adequate, whether new programmes are required, and whether performance issues can be addressed through training) and strategic (identifying knowledge, skills, and attitudes that will be needed in the future).[9] By asking participants about their specific challenges and expectations from the workshop, facilitators address the principles of relevance and self-direction, as outlined in the theory of andragogy.[10]

The **planning and designing** stage focuses on developing effective learning strategies to address the gaps identified in the needs assessment stage. This involves managing administrative aspects of training; preparing curricula, materials, and learning aids; defining success indicators, learning objectives and outcomes; and planning and developing a monitoring and review process to assess whether learning objectives have been achieved.[11] Incorporating case studies, dilemmas, and scenarios that reflect real-life situations addresses the desire of adult learners to be acknowledged for their experiences and provides an opportunity to critically reflect and brainstorm solutions.[12]

9 Costa and Thorens, *Training Manual on Police Integrity*.

10 Irina Ketkin, 'A Comprehensive Guide to Adult Learning Theories', The L&D Academy (7 November 2023, updated 19 October 2024), https://www.theIndacademy.com/post/a-comprehensive-guide-to-adult-learning-theories

11 Costa and Thorens, *Training Manual on Police Integrity*.

12 Ketkin, A Comprehensive Guide to Adult Learning Theories.

Delivery and implementation is the most 'visible' stage of the learning cycle, as the developed strategies are put into practice and presented to participants. This stage involves managing the learning environment and creating favourable conditions for participants to achieve the established learning objectives. Notably, only about 20 per cent of the total time is spent on actual delivery, while the remaining 80 per cent is devoted to preparation – much like the unseen bulk of an iceberg.[13] When introducing new concepts throughout the training, always connect them to participants' current roles, in order to demonstrate the applicability of new knowledge.[14]

The **reviewing and evaluating** stage is aimed at revisiting the existing strategy and making corrections and improvements for preparing the next training cycle. It is important to remember that training is successful only when it results in the transfer of knowledge, skills, or behaviours to practice.[15]

Further details on adult learning theories and learning styles can be found in Annex II.

13 Costa and Thorens, *Training Manual on Police Integrity*.

14 Ketkin, A Comprehensive Guide to Adult Learning Theories.

15 Costa and Thorens, *Training Manual on Police Integrity*.

Facilitators' techniques and tips

The following section explores some techniques and tips which facilitators can use when conducting training.

Learning interventions

Learning and training are not the same. Learning on both individual and organizational levels can occur even without engaging in formal training programmes – through experience, self-instruction, or reflection. Training, however, remains a common strategy for addressing various defence ethics issues. This section explores several key training methods.[16]

Lectures

The lecture is the most traditional and widely used training method. Its main advantage lies in its cost-effective delivery of information to large groups. Typically, a lecture involves one-way communication from a qualified or experienced speaker to the audience. Although it may offer limited opportunities for discussion or interaction, a lecture is a convenient way to introduce either basic or advanced information and set the context for further discussion. Ideally, a lecture should be complemented by other training methods to facilitate engagement.

Focus group discussions

A focus group discussion involves structured, interactive dialogue centred on a specific question or set of questions. Guided by a facilitator, participants are encouraged to share their views and experiences. This method promotes active learning and enhances knowledge retention by allowing all members to contribute to the discussion.

Plenary panels

A plenary panel consists of several experts or individuals offering different viewpoints on a particular issue. This method is effective for presenting a range of perspectives and stimulating further discussion in seminars and workshops. It is well suited to large audiences (50–100 participants) and is frequently used to conclude workshops or a series of classes. It allows for broad reflection and the synthesis of ideas. Ideally, participants should have the opportunity to ask questions and engage with panel members before the session concludes.

16 DCAF, *Toolkit on Police Integrity*.

Poster presentations

A poster presentation involves a visual display of material that has been designed and organized by participants – often through posters or PowerPoint slides. This method encourages learners to engage creatively with the training topic by summarizing and presenting key concepts in a visual format.

Case studies

The case study method is widely used in adult learning and professional education. Its primary strength lies in real-life examples that illustrate key issues in practice. Often, the cases presented are well known or relevant to the participants, allowing them to draw upon their own experiences, contribute insights, and engage in meaningful discussion. Because case studies reflect actual workplace situations, learners tend to view them as highly relevant and engaging.

Role play

Role play involves participants acting out realistic scenarios in which they assume specific roles. Roles are typically assigned without prior preparation to encourage spontaneity and authentic responses. This method is particularly effective for developing empathy, communication skills, and situational awareness. Following the enactment, a group discussion is usually held to reflect on the experience, analyse participants' responses, and draw lessons from the exercise.

Simulations

A simulation shares many features with role play but aims to recreate real-world conditions more accurately. It is designed to immerse participants in a lifelike scenario that closely mirrors the complexity of an actual professional situation. For example, a simulation might involve an officer being offered a bribe by a member of the public, requiring an immediate ethical and procedural response.

Tactical decision games/scenario-based training

This method represents a highly realistic form of simulation, designed to replicate the psychological and operational environments in which participants must make critical decisions. Originally developed for critical incident training, this approach focuses on non-technical skills, such as judgement, decision-making, and emotional control, under conditions of stress and uncertainty. Furthermore, a game allows experimentation, reduces social desirability bias, and encourages participants to express genuine ethical doubts. Ethics always has a personal dimension; if participants cannot voice their real doubts, ethical training loses its meaning.

Brainstorming

Brainstorming aims to generate a wide range of creative ideas within a short time. It encourages innovation, challenges 'groupthink', and exposes participants to new perspectives beyond their usual experience. A facilitator ensures equal participation, keeps the atmosphere open and non-judgemental, and prevents rank from influencing the process. Ideas are recorded on whiteboards, posters, or digital tools, and then grouped into themes for presentation and discussion. Including someone from a different professional background can add valuable insights.

Six category intervention analyses

Designed by John Heron (2001), this concept identifies six fundamental types of interventions that facilitators can use in the classroom to address learners' psychological needs during a session.[17] These interventions, as shown in Table 1, are broadly categorized into two groups: (a) authoritative and (b) facilitative and are often considered complementary to the ideas of learner-centred and teacher-centred approaches.

Table 1. John Heron's authoritative and facilitative interventions

Authoritative interventions	Facilitative interventions
Prescriptive intervention, as the name suggests, involves the facilitator providing advice, a plan of action, training objectives, and rules that guide the behaviour of the entire class.	**Cathartic intervention** enables participants to release emotions, promoting self-reflection and self-discovery. By asking questions, encouraging experience-sharing, and exploring solutions, the facilitator helps participants solve problems in new ways.
Informative intervention is less directive than the prescriptive approach. It is aimed at sharing useful ideas, concepts, and case studies with participants. However, facilitators should be careful not to over-teach, as attention spans typically start to decline after about 20 minutes.	**Catalytic intervention** is aimed at fostering self-awareness and reflection, helping participants become more self-directed in their decision-making process.
Confronting intervention occurs when a facilitator helps participants recognize limiting attitudes or behaviours they may be unaware of. It is not about 'attacking' but rather about guiding participants to identify their existing blind spots.	**Supportive intervention** is used to acknowledge the value of individuals, as well as demonstrating understanding and support. This can be achieved through comments and feedback that validate experiences without trivializing them.

17 Costa and Thorens, *Training Manual on Police Integrity*; Nick Bolton, 'Expanding Your Supervision Range: Using Heron's 6 Categories of Intervention in Coaching Supervision', International Centre for Coaching Supervision (7 June 2020), https://iccs.co/herons-6-categories-of-intervention-in-supervision.

Asking questions

Asking questions[18] is a crucial tool in the learning process, as it allows us to navigate complexities, clarify points, examine how we assign meaning to information, review our perspectives, consider alternatives, identify internal contradictions, and evaluate the accuracy of information.

Questions can be classified in two types: closed questions and open-ended questions. While the first type of question usually entails a 'yes' or 'no' response, the second type of question encourages reflection and gives respondents freedom in shaping their answers. Facilitators are encouraged to use a mix of both types, as this involves combining the assessment of knowledge ('lower-order thinking' or closed questions) with evaluation of the ability of participants to apply, analyse, synthesize, and evaluate information and concepts ('higher-order thinking' or open questions).

Re-directing is also an important technique that facilitators can use. When a participant poses a question, instead of responding immediately, the facilitator can open the floor to the group, giving others the opportunity to respond.

Recognizing one's limitations from the outset is crucial: a facilitator is not there to act as a 'know-it-all'. Instead of providing a potentially incorrect response, it is better to revisit the question at a later point, after researching relevant information. Indeed, the main goal is not to showcase the facilitator's knowledge, but to provide a platform for exchange between participants and to encourage collaborative learning.

18 Costa and Thorens, *Training Manual on Police Integrity*.

01

Ethics, law and culture in the defence sector

Just because you're right doesn't mean I'm wrong.

Module objectives

To develop participants' understanding of the distinction between personal morality and institutional ethics in defence settings, and to explore how legal frameworks, cultural norms, and ethical standards interact in shaping professional conduct. The lesson aims to equip defence personnel with the knowledge and critical thinking skills needed to recognize and respond to ethical dilemmas, uphold institutional integrity, and maintain public trust in democratic societies, particularly in culturally diverse and post-conflict environments.

Key information

a. Ethics is properly concerned with what we should do, how we ought to act, and where to orient our actions. Philosophers and legal scholars often use the terms 'ethics' and 'morality' interchangeably; however, in military settings it is useful to distinguish between them. Morality (or 'morals') reflects an individual's internal values and upbringing, while ethics refers to the shared professional standards that guide conduct within an institution – in this case, the armed forces.

b. The legitimacy of the defence sector in democratic societies depends on its adherence to both the law and ethical norms. Citizens grant extraordinary powers to the military, including the right to use force in exchange for lawful and ethical conduct. Legal compliance is therefore a condition for public trust. Without it, defence institutions risk losing legitimacy, both domestically and internationally. The law can, however, contradict ethics and create uncertainties.

c. Culture plays a significant role. In some cultures, hierarchical authority discourages the questioning of superiors, even on ethical grounds. In other cultures, traditions of open dialogue and individual responsibility prevail. These differences shape how personnel handle dilemmas, report misconduct, and uphold integrity.

d. Corruption is another area where cultural norms heavily influence ethical behaviour. In countries where nepotism, favouritism, or informal networks are culturally tolerated or even expected, defence institutions may struggle to enforce transparency and merit-based systems.

e. While illegality in the defence sector can be prosecuted through legal systems, unethical behaviour requires a broader institutional and cultural response. Strengthening both legal compliance and ethical standards is essential for ensuring the integrity of defence institutions, especially in conflict-affected or post-authoritarian contexts. Addressing unethical conduct requires institutional and cultural transformation beyond legal remedies. Building both legal compliance and ethical resilience is crucial for legitimacy, particularly in fragile or transitioning states.

Module content

Morality, ethics, human rights, law, and culture in the defence sector

Reflection on the world and on human conduct reveals a continual potential for improvement. This is the realm of ethics. Ethics concerns not how things *are*, but how they *ought to be*. It rests on the human capacity to evaluate actions and discern what is right, just, and virtuous, irrespective of prevailing behaviour or circumstance. In this sense, ethics embodies a hierarchy of values – good and bad, right and wrong, admirable and deplorable, virtuous and corrupt.

The difference between morality and ethics

In the defence context, many people associate morality with personal beliefs – for example, 'I believe that using lethal force outside combat is wrong.'

While philosophers and legal scholars often use the terms ethics and morality interchangeably, in military settings it is useful to distinguish between them. Morality reflects an individual's internal values and upbringing, while ethics refers to the shared professional standards that guide conduct within an institution – in this case, the armed forces.

This distinction helps explain why we speak of military ethics or codes of conduct rather than 'military morality': ethics provides a framework for professional behaviour that may at times require individuals to act beyond – or despite – their personal moral intuitions.

It is sometimes argued that there is nothing universal in ethics, and that one's values and moral codes are determined by one's culture. This position is known as 'relativism': whether an action is right or wrong depends on the norms of the society in which it is practised. The differences we observe among cultures make relativism seem plausible. What is morally acceptable varies with place, culture, and time: bribery, genital mutilation, slavery, nepotism, human sacrifice, child labour, eating animals, and so on have all been practised and approved of in some places, but reviled in others. The relativist concludes from this that there are no universal moral principles.

Aiming at what is better rather than what is worse is another approach to decide what is right and what is wrong. It follows as a moral principle that our actions *should aim* at maximizing happiness and minimizing suffering. By this reasoning, the *consequences* or *results* of an action determine whether it is right or wrong. Philosophers call this principle 'utilitarianism': an action is morally right if it maximizes the benefits for those affected by the action. This is an *objective* moral principle in that we will arrive at it regardless of the cultural perspective we take. But obtaining good consequences is not the only moral consideration.

Imagine, for example, that a soldier is in hospital for surgery on a torn Achilles tendon. While the soldier is on the operating table, the surgeon is told something remarkable about this patient's laboratory tests: they happen to be a tissue match for four different military patients in that same hospital who are about to die unless they receive organ transplants. One patient needs a liver, one needs a heart, one needs a lung, and one needs a kidney. If the surgeon were to harvest these organs from the Achilles tendon patient and perform these four transplants, the surgeon could save four lives. Would this be morally right? If we were to apply only the principle of utilitarianism, the answer would be yes. Although the patient with the torn Achilles tendon would die, we would be maximizing the overall benefits for those four patients taken as a whole, all who were affected by the surgeon's action. Of course, operating on a healthy person and harvesting their organs without their consent strikes us as morally repugnant.

This example indicates that utilitarianism – aiming at maximally beneficial results – captures only part of the moral picture. It does not capture our sense that there is something precious and inviolable about each human individual which cannot rightly be overridden, even if doing so produces aggregate benefits. This notion that human individuals are intrinsically valuable and must be respected as such goes by the name 'human rights'. Unfortunately, this term is used in so many different ways that the concept seems vague. Here is what we mean by rights in the context of ethics; humans have the ability to choose not only what to do, but also what principles they will follow. This is what we mean by 'autonomy'. The word 'autonomy' comes from the Greek *autos*, meaning 'self', and *nomos*, meaning 'law'. Humans are able to

choose for themselves a law or principle to which their actions conform. A bear who attacks an intelligence officer in the woods is not deliberating about which law to choose to govern his actions, nor about exercising free will, nor acting on principle. The bear is not an autonomous being, one to whom we would attribute moral responsibility. By stark contrast, we humans would be held morally responsible for how we treat the very same intelligence officer. Again, the difference is that humans have the rational capacities that enable us to deliberate, to restrain our actions in accordance with self-chosen principles (rather than mere instinct), and to exercise free will. We might even say that is what *makes us* human: free will, rationality, and autonomy differentiate us from the rest of creation. And this ability to guide our own conduct confers upon humans a unique dignity and value.

While we've explored the foundations of human rights, they are to be translated into simple moral guidance, such as the 'Golden Rule': do to others what you would have them do to you. We may be most familiar with the Christian formulation of the principle, but versions can be found in every religion, including Judaism and Islam, and almost every culture. The simplest way to determine if you are respecting the rights of others is simply to apply this test.

Why is professional ethics important?

Based on experience, one might at times reach the discouraging conclusion that ethics holds little practical significance. This perception is reinforced by the disparity often observed between the proclamations of certain leaders and their actual conduct, particularly in matters related to ethical governance and accountability.

In early 2025, a senior political leader suggested that the continuation of external assistance to a conflict-affected state could depend on securing access to that state's valuable natural resources, such as rare earth materials.

In fact, about the only thing that people seem to agree on is the belief that *'ethics' is, finally, a matter of personal or cultural opinions* about right and wrong. This process illustrates the essence of ethics: reflecting on practice to define acceptable conduct and aspirational standards.

Members of a professional community, engaged in a common enterprise such as defence of the nation and its citizens, are less free to 'go their own way' with respect to moral beliefs. *They share a conception of the Good* at which their common professional activity aims – for example, the security of their citizens. They are thus compelled (whether they wish to or not, or always realize it or not) to engage with each other in a search for better or worse means of attaining or achieving those ends.

Assuming only a good-faith commitment to the practice of their profession, the members of that profession are thereby compelled to engage with each other on the *proper practice* of their profession. They are led to generate a common code of practice, and ideals of best practice. And often, in reflecting upon some of the worst tragedies and disasters that befall individual members of their profession, they are led further to specify clearly the boundaries of acceptable professional practice, and the definition(s) of *professional malfeasance*. But *that is precisely what ethics itself is:* the discernment of the *limits* on acceptable conduct, through reflection upon our practices as well as upon *the standards and ideals* upheld within the best practices of our profession.

We are entitled to hold ourselves accountable for living up to these standards, or, when required, to sit in judgement of those who fail to do so. There is nothing self-righteous or sanctimonious about *demanding that we all live according to the rules, laws, and ideals to which we have all voluntarily agreed, and that we all have freely shared in forging.*

Why we must address the law

While ethical behaviour can be guided by moral principles, institutional culture, and professional codes, it is the legal framework that provides the essential structure for accountability, transparency, and legitimacy in the defence sector. In this context, law not only restrains abuse of power but also embeds ethics into the core functions of military and defence institutions. Law defines the boundaries of acceptable conduct. For instance, International humanitarian law (IHL), military codes of justice, and national legal systems codify rules on the use of force, the treatment of combatants and civilians, and the protection of human rights. These legal standards are not mere technicalities; they are ethical commitments enshrined in binding norms. For example, the Geneva Conventions limit what is permissible in armed conflict, ensuring that military necessity is balanced with humanity. Compliance with such laws reflects ethical behaviour at both individual and institutional levels. Law enforces accountability, whereas, in the absence of legal mechanisms, ethical violations in the defence sector often go unpunished. Moreover, law shapes organizational culture and leadership norms. Defence institutions are hierarchical and often operate under secrecy. So, legal requirements such as anti-corruption regulations, whistle-blower protections, and codes of conduct serve as formal tools for promoting transparency and ethical integrity. When integrated into training and doctrine, legal norms become part of the professional ethos of military service.

However, the relationship between law and ethics is not without conflict. Legal requirements or the ‘letter of the law’ may be seen as falling short of the ‘spirit of the law’ or the ethical norms underpinning the law. For example, a senior military official assumes a position in a defence industry company only two years after leaving active service. In his previous role, he was responsible for overseeing contracts with that same company, which subsequently received significantly increased business from the military institution. Although post-service employment is not prohibited, such circumstances may give rise to ethical concerns and potential questions regarding integrity and conflict of interest (COI). It creates a perception of a system where decisions may be influenced by personal gain rather than public interest.

There are instances where legal compliance may fall short of ethical expectations, such as the use of lethal force in legally justified but morally questionable circumstances. In one instance, an airstrike conducted during counterterrorism operations targeted a vehicle believed to be associated with an armed group. Subsequent investigations revealed that the intelligence was flawed and the attack resulted in civilian casualties, including children. The operation was later described as an ‘honest mistake’, attributed to procedural and communication failures, and no disciplinary action was taken. While the action was deemed legally permissible under the law of armed conflict (LOAC), it sparked widespread criticism from human rights organizations and lawmakers, who argued that the lack of accountability perpetuates a culture of impunity and fails to address systemic issues in drone warfare.

Rigid adherence to military protocols may at times hinder moral courage or discretion in complex operational settings. In one instance, low-ranking officers and soldiers witnessed abuse of detainees but did not report the misconduct immediately, citing procedural limitations (military protocol required personnel to report incidents through their immediate superiors) and fear of violating the military chain of command. It highlights that even where officers/soldiers understand their rights to disobey an illegal order or report, organizational culture can be a source of tremendous pressure that ultimately prevents reporting of misconduct. While legal compliance with command structures was maintained in this example, it discouraged ethical whistle-blowing, illustrating how strict rule-following can sometimes suppress moral courage in high-stakes environments.

Illegal conduct vs unethical behaviour

In the defence sector, distinguishing between illegal conduct and unethical behaviour is vital to maintaining governance, accountability, and public trust. **Illegal conduct** violates national or international law and carries criminal or administrative penalties. Examples include bribery in procurement, falsifying invoices, theft of military supplies, unlawful detention, or the use of prohibited interrogation methods. In conflict situations, violations of IHL such as targeting civilians or mistreating prisoners also constitute criminal offences.

Unethical behaviour, while not always illegal, undermines institutional integrity and professionalism. Practices such as favouritism, nepotism, or COI weaken meritocracy and trust. Moral disengagement such as dehumanizing civilians or adversaries can normalize abusive conduct, while disrespectful workplace cultures marked by bullying, harassment, or discrimination erode morale.

Culture

Ethical behaviour in the defence sector is shaped not only by laws and regulations but also by culture. Culture plays a powerful, often subtle, role in shaping decision-making, leadership, accountability, and attitudes toward rules and authority. In the defence sector, where decisions often involve life, death, secrecy, and national interest, cultural influences can either reinforce ethical standards or undermine them.

Cultural norms shape behaviours that can be misunderstood unless military leaders and personnel are trained to recognize cross-cultural differences in communication, hierarchy, and expressions of respect. In many Western military cultures, direct eye contact is seen as a sign of confidence, respect, and honesty. A subordinate who avoids eye contact with a superior might be perceived as evasive, insubordinate, or lacking in professionalism.

However, in several Asian and Middle Eastern cultures, avoiding eye contact with a superior is actually a sign of respect and humility. Direct eye contact may be considered confrontational or disrespectful, especially in hierarchical relationships. A soldier from such a background might lower their gaze when speaking to an officer as a culturally appropriate gesture – but this could be misinterpreted in a multinational force.

In some societies, respect for authority is deeply ingrained, and challenging a superior even on ethical grounds may be viewed as disloyal or disrespectful. In other societies, there may be stronger traditions of open debate and individual conscience. These cultural differences affect how defence personnel respond to ethical dilemmas, how they report misconduct, and how institutional integrity is upheld. Cultural norms can also normalize corruption. In countries where nepotism, favouritism, or informal networks are culturally tolerated or even expected, defence institutions may struggle to enforce transparency and merit-based systems. For example, appointing relatives or friends to key positions in the defence hierarchy may be seen as normal in some cultural contexts, even though it undermines professional standards and institutional credibility.

On the positive side, culture can be a powerful driver of ethical excellence in defence institutions. Military traditions that honour integrity, courage, and service can instil a strong sense of duty and moral responsibility.

> Therefore, promoting ethics in the defence sector requires not only internal reforms but also cultural change at the national level – through education, civic engagement, and public accountability.

Importantly, the defence sector often inherits and reflects the broader societal culture. If society at large struggles with rule of law, inequality, or low public trust in institutions, these challenges are likely to manifest within the military as well. Therefore, promoting ethics in the defence sector requires not only internal reforms but also cultural change at the national level – through education, civic engagement, and public accountability.

Multinational operations further complicate the cultural landscape. Peacekeeping missions, coalitions, and joint training exercises bring together defence personnel from diverse cultural backgrounds. Ethical standards may differ, and cultural misunderstandings can lead to friction, misconduct, or mission failure. Building shared ethical norms in such contexts requires cultural sensitivity, mutual respect, and clear codes of conduct that transcend national differences.

Remember that

- ✓ Ethics = shared standards; Morality = personal values
- ✓ Defence legitimacy depends on lawful and ethical conduct
- ✓ Culture influences accountability and reporting behaviour
- ✓ Permissive corruption norms undermine integrity
- ✓ Ethical strength requires institutional and cultural reform

Check-your-skills exercises

Task 1. Card game: 'Illegal or unethical?'

Objective: Participants will analyse real-world defence-related workplace scenarios and decide whether each situation constitutes an illegal act or unethical behaviour.

Target group: Military or defence personnel, civil servants, integrity officers, or participants of defence training courses.

Materials needed:

- Printed cards (9 total; see Fig. 2)
- Two signs for the different categories: 'Illegal' and 'Unethical'
- Pens/paper for group notes

Instructions:

1. Divide participants into small groups (3–5 people per group).
2. Shuffle and then distribute one or more cards per group.
3. Each group reads the scenario and discusses whether it represents an illegal act or unethical behaviour.
4. The facilitator walks around the room, listening to discussions and prompting critical thinking.
5. After 15–20 minutes, regroup and go through each scenario together.
6. The facilitator invites groups to justify their choices and briefly explains the correct classification with reference to defence norms/law.

Facilitator tip: Encourage participants to reflect not only on the legal classification, but also on the organizational culture that allows these behaviours and how they could be addressed proactively. Wherever possible, it would be helpful to emphasize clearly that this is not just about upholding ethical standards – unethical behaviour directly undermines operational effectiveness.

Extension option: Use coloured cards or icons (e.g. shield for illegal, compass for unethical) to visually reinforce categorization when printing.

You discover that a fellow officer accepted money from a candidate to influence the outcome of a recruitment board for military service.

Is this illegal or unethical – or both? What are the consequences in a military context?

You learn that your commanding officer appointed their relative to a strategic planning role without any formal vetting or qualification review.

Is this illegal or unethical – or both? How might this affect operational integrity?

A logistics officer knowingly approved the procurement of substandard body armour for active units.

Is this illegal or unethical – or both? What risks does this pose for personnel and mission success?

You see your superior officer submitting fraudulent travel expense reports for training missions that never took place.

Is this illegal or unethical – or both? What systems could catch or prevent this?

A non-commissioned officer regularly uses a military transport vehicle for family errands and personal use.

Is this illegal or unethical – or both? Where is the line between privilege and abuse?

Your department signs a high-value weapons contract, and you learn the supplier paid bribes to senior defence staff to secure the deal.

Is this illegal or unethical – or both? How should this be reported and investigated?

You observe fellow service members drinking alcohol during daytime hours while on active duty at a secure base.

Is this illegal or unethical – or both? How does this affect safety and discipline?

During a training exercise, a senior officer repeatedly humiliates a subordinate in front of the platoon for making mistakes.

Is this illegal or unethical – or both? Where does tradition and discipline end and abuse begin?

Some unit members call a colleague by an offensive nickname. The colleague insists they are okay with it, but other members of the unit appear uncomfortable.

Is this illegal or unethical – or both? How should leadership assess the true impact of such behaviour?

Figure 2. Cards to be used in the 'Illegal or unethical?' card game

Task 2. Manipulation with legal norms

Description of situation:

An officer employed by a defence agency via employment company was dismissed due to a breach of integrity. Upon termination of employment, he was expected to return his official laptop. He refused to do so, however, claiming he had never received such a device. According to the national legislation of the country where he was employed, individuals are required to sign for any official equipment issued to them. In this case, the organization, operating on the basis of trust, did not require a signed acknowledgement upon issuing the laptop.

Timeline:

1. Letter of non-renewal of contract (1 December 2024)

Dear Sir,

I am writing to formally inform you that your contract concluded with XXX acting on behalf of YYY will not be extended beyond its current expiration date.

In accordance with organizational policy, and considering that YYY will be closing offices for the holiday season, we kindly request that you return all YYY-owned equipment and material to XXX by 31 December 2024. This includes, but is not limited to, your YYY-assigned laptop, computer monitor(s), and any other equipment or materials in your possession that belong to the organization.

2. Letter from XXX employment company informing of non-return of assigned laptop and other equipment (January 2025)

My colleague met with the officer at the end of December, and that's when the employment record book was handed over to him. Since it was December, the officer said he still needed the computer for work and would return it in January.

I wrote to him several times on Viber – he read the messages but didn't respond. Recently, I called him and asked him to return the computer, to which he replied: 'You never gave it to me, so I have no reason to return it to you.'

3. Reminder was sent to the officer to return the equipment that belongs to the organization (January 2025)

4. Response received from the officer (February 2025)

I was shocked to receive your email, as I've never received any laptops, equipment, etc. from the organization, thus I kindly ask you to provide me with relevant papers/legal documents confirming this. Otherwise, I don't understand what you're talking about, and I totally reject all your claims as groundless, illegal, and unlawful.

Activity:

Please review the situation in light of the email correspondence provided and assess whether the officer's conduct can be considered legal and ethical under the applicable legal framework and professional standards.

Work in pairs or small groups and respond to the following prompts:

Factual review:

- Which facts are uncontested?
- What evidence (written or verbal) supports either party's claim?

Legal assessment:

- Based on standard employment and property law, is the officer legally obliged to return the equipment?
- Could the officer's refusal constitute misconduct, breach of contract, or criminal offence (e.g. theft, conversion of property)?

Ethical assessment:

- Is the officer acting in accordance with professional military or civil service values (e.g. integrity, accountability, responsibility)?
- What alternative actions could the officer have taken to clarify or resolve the matter ethically?

Organizational risk and response:

- What risks does this behaviour pose to the organization (security, operational, reputational)?
- What procedural safeguards (e.g. handover protocols, equipment registers) could prevent such disputes?

Outcome recommendation:

- What would be a reasonable disciplinary or administrative outcome based on this behaviour?
- Should this be pursued as a legal case or resolved internally?

02

Ethics and leadership in the defence sector

Leadership is not about self. It is about purpose, service, and others.

– General Stanley McChrystal, Team of Teams (2015)

Module objectives

To understand the ethical decision-making and adaptive leadership in complex defence environments, and to explore how future challenges require leaders who combine values with modern skills.

Key information

a. Ethics as the core of leadership. Leadership in the defence sector is fundamentally about service to others, not about personal gain. Ethical leaders put mission, people, and purpose ahead of self-interest. They consistently strive for the common good, treating each soldier or civilian with dignity and respect, regardless of rank. Integrity is the bedrock of effective leadership: without it, there can be no trust, and without trust, command authority collapses. An ethical leader inspires confidence both upwards and downwards in the chain of command.

b. Qualities of an ethical leader. They demonstrate professionalism by being consistent in words and actions, transparent in decision-making, and empathetic in dealing with subordinates. Ethical leaders must also balance traits: confidence with humility, initiative with accountability, boldness with prudence. These qualities help them adapt to complex situations while setting a moral example for others to follow.

c. Leadership dilemmas. Leaders often face dilemmas that pit equally important values against each other:

- **Loyalty vs professionalism:** Loyalty ensures unity and trust, but professionalism guarantees competence and effectiveness. The most effective leaders find a balance, embodying loyalty to the nation and laws while continuously developing professional skills.
- **Born vs trained leaders:** Some argue that leadership is innate, others that it can be taught. In practice, natural talent may help, but training, education, and experience are essential in modern contexts. Leaders must invest in developing themselves and their subordinates to sustain effective leadership across generations.

d. Future warfare challenges. The environment of future warfare will be shaped by demographic pressures (population growth, urbanization, resource scarcity) and technological advances (artificial intelligence (AI), drones, quantum computing, advanced sensors). Leaders will face time pressure, information overload, and complex operational environments. In such circumstances, decision-making must be rapid but also ethically sound, legally correct, and morally defensible. Preparing leaders for these challenges requires new approaches to education, continuous training, and war-gaming exercises that simulate uncertainty and complexity.

e. The role of NCOs. Non-commissioned officers (NCOs) function as the primary custodians of ethical conduct within units. Through daily interaction with soldiers, they model professional behaviour, address misconduct early, and ensure that ethical standards are upheld even under pressure. By reinforcing norms of integrity, accountability, and respect, NCOs help to create a command climate in which soldiers understand both what is expected of them and why ethical discipline matters. Their leadership contributes to resilient values-based organizations where responsibility and initiative are distributed across all levels.

f. Civilian vs military leadership. Civilian and military leaders share core ethical values but operate within distinct institutional cultures. Civilian leaders emphasize democratic legitimacy, oversight, accountability, and transparency in defence governance. Military leaders, meanwhile, emphasize discipline, duty, cohesion, and operational effectiveness within hierarchical structures. Ethical conflict may arise, but this balance is healthy: civilian leaders provide political vision and oversight, while military leaders bring professional expertise and operational integrity. Both roles are complementary and essential to a legitimate and effective defence system.

g. Meritocracy and leadership development. Future military effectiveness depends on meritocracy – promoting the best individuals based on talent, character, and commitment rather than privilege or personal connections. This principle builds trust within the ranks and ensures capable leaders are positioned where they are most needed. Education, professional training, and innovative methods such as war-gaming need to prepare leaders for unknown challenges, while career development systems must create opportunities for those who demonstrate potential. Ultimately, the key to ethical leadership is continuous investment in people, nurturing their growth and empowering them to take on greater responsibility.

Module content

The ethical leader

The ethical leader will always (1) seek the common good while (2) treating each individual – from the lowest soldier in the chain of command to the highest – as the leader himself would want to be treated: as an irreplaceable, intrinsically valuable person, deserving of respect.

There's no shortage of literature about leadership but because it's a personal thing, essentially it's about you and your behaviours and at its most simple it's about translating your intent into action through other people. So here are a few things that have helped me: At its heart, sits moral courage, mutual respect, comradeship and self-discipline. This builds trust, without which there can be no leadership. The hallmarks of successful military leadership also include initiative, daring, self-confidence, professional knowledge and energy. An inextinguishable will to win combined with a determination not to be frustrated by the inevitable setbacks and matched with a preparedness to experiment and innovate in order to learn. Leadership and learning go hand-in-hand, along with a relentless pursuit of professional excellence. It helps if you have the confidence to encourage an open, collaborative and challenging culture coupled with the patience to tolerate the honest mistakes of subordinates in order to develop their confidence, initiative and experience. You're trying to bring out the best in people. I have always tried to place a premium on decentralisation and delegation, intelligent co-operation, speed of action and low-level initiative. People enjoy freedom, not micromanagement. Finally, an irrepressible sense of humour, proportion and humility goes a long way in nurturing the tenacity, resolution and fighting spirit which is what we are all about and keeps everyone going in adversity. The martial spirit of our soldiers is the only true test of our readiness. Keep that bright, and in my experience, the rest will follow.

Carleton-Smith, M, 'Reflections on Leadership and Geopolitics with Sir Mark Carleton-Smith', The Minter Dialogue Podcast (16 March 2025). Available at: https://www.minterdial.com/2025/03/mark-carleton-s-smith

The ethical leader will be trustworthy, courageous, fair, disciplined, caring, and loyal. They will display professionalism, consistency, transparency, and, above all, integrity, thus setting an excellent example for others to follow.[19]

Ethical leadership demands

Intellectual capacity: Professional competence, decisiveness, and adaptability

Traits of character: Integrity, courage (physical and moral), resilience (physical and mental), confidence, commitment, and discipline

Social skills: Empathy, compassion, and the ability to communicate and inspire.

Moral standards are higher for the character of the military professional than they would be for the average citizen for a number of reasons. First, the military professional is entrusted with the use of lethal weapons and has been trained to use violence. Such power in the hands of an immoral person would endanger innocent people. Second, command authority depends not just upon holding a rank, but on having the kind of character your subordinates know they can rely upon. If a subordinate doubts that a commanding officer has a good character, they might be hesitant about following orders. Simply put, the military professional operates within a chain of command, and that chain operates on trust; trust both up and down the chain of command is necessary for the chain to be effective. There is yet a third reason why good character is essential for members of the military: they are the representation of the nation which they serve. If a nation at war is to maintain the moral high ground, its soldiers must be above reproach. A soldier can credibly defend moral values on the world stage only if their own character and conduct embody those same values. Ethical behaviour therefore becomes a strategic asset: it underpins the legitimacy of military operations, strengthens the credibility of national commitments, and reinforces adherence to international norms.

Future warfare: a very different environment

Warfare in the future will take place in a radically different environment, shaped by global trends and technological advancements. Demographic changes such as population growth, rapid urbanization, uneven economic development, and resource shortages will all influence the context of conflict. At the same time, the rapid development of technologies, including AI, unmanned aerial vehicles, quantum computing, and advanced sensors will have specific impacts on decision-making, command structures, or autonomy. In this environment, new leaders will face immense challenges: constant time pressure, overwhelming flows of information, and the complexity of intense operations. These pressures demand not only quick thinking but also commitment to ethical decision-making. Leaders will be expected to act responsibly, always making decisions that are both legally sound and morally right. However, rapid decision-making may risk ethical compromise unless leaders are deliberately trained to withstand that pressure. To prepare for the unknown, education, training, and war-gaming will be critical tools for building readiness and resilience. Leadership development must therefore integrate values such as integrity, courage, and responsibility with technological proficiency, ensuring that leaders are equipped for both human and digital dimensions of warfare. In this regard, the question of selecting and training suitable leaders is growing in importance as well.

19 Rear admiral Robert Hranj held a presentation on military leadership in Yaremche, Ukraine in August 2025, where these ethical leadership challenges and demands were discussed. The training was based on the current toolkit.

At the core of this vision is meritocracy: the principle that the best must be promoted. By identifying and empowering those with the greatest talent, skill, and commitment, armed forces can build leadership that is capable of navigating the complex and unpredictable challenges of future warfare. It is not easy, however, to overcome institutional barriers and biases.

Civilian vs military leaders in the defence sector

Military leaders and civilian ministers of defence, deputy ministers, and political directors are guided by core ethical values that define the legitimacy, integrity, and accountability of the defence system. At the core, both military and civilian leaders are bound by a shared commitment to serve the national interest, uphold the rule of law, and protect the lives and rights of citizens. Their ethical codes emphasize values such as integrity, loyalty, responsibility, and public service. Both types of leaders are expected to act with impartiality and professionalism, especially in matters of national security, where misuse of authority can have severe consequences. Additionally, both are accountable – though in different ways – to democratic institutions and the public. Ethical governance in defence relies on transparency, respect for human rights, and accountability mechanisms that apply to both civilian and military actors. Whether shaping policy or commanding troops, both must resist corruption, avoid conflicts of interest, and act with a strong moral compass in the face of complex dilemmas.

Despite these shared foundations, the ethical values of military and civilian leaders often stem from distinct institutional traditions. Military leaders are typically guided by codes of military ethics, emphasizing duty, honour, discipline, courage, and obedience. Their decisions are framed within a hierarchical structure where orders must be followed, often under extreme conditions. In this environment, loyalty to command, unit cohesion, and operational effectiveness are core ethical pillars. Military leaders also confront unique moral challenges such as the use of lethal force, protection of civilians during conflict, and treatment of prisoners, which demand strict adherence to IHL and the law of armed conflict.

In contrast, civilian leaders operate within a political and legal framework where democratic legitimacy, civilian oversight, and public accountability are paramount. Their ethical obligations are broader and often more abstract: ensuring that defence policy reflects democratic values, managing public resources responsibly, and maintaining transparency in decision-making. Civilians must also balance competing interests (political, diplomatic, economic), requiring ethical judgement that navigates both national and international expectations.

The relationship between military leaders and civilian ministers of defence is not without ethical tensions. Military leaders may view political decisions as disconnected from operational realities, while civilians may perceive the military as resistant to reform or excessively secretive. Ethical friction can emerge around issues such as use of force, treatment of whistle-blowers, or transparency in military spending.

However, these tensions are also a source of balance and ethical complementarity. Civilian leaders bring democratic oversight and political vision; military leaders contribute professional expertise and operational integrity. Mutual understanding and institutional respect – not just individual ethical conduct – are essential to maintaining both effectiveness and democratic legitimacy in defence governance.

Dilemmas of leadership

One of the enduring dilemmas in leadership, particularly in times of crisis, is whether to prioritize loyalty or professionalism when selecting leaders. Loyalty and professionalism are not mutually exclusive but may come into conflict in high-stakes environments, particularly during leadership selection. This question is especially relevant in military and security contexts, where both qualities are essential but can sometimes appear to conflict with each other.

From one perspective, loyalty must come first: *'I would choose a loyal person – loyal to their country, constitution, and laws. There is always time to train and develop them, allowing them to gain professional and life experience.'* This argument highlights that loyalty is the foundation upon which all other qualities can be built, because a leader who lacks loyalty to the mission, the institution, or the values it represents may undermine morale and cohesion, regardless of their technical competence.

Others have stressed that the answer depends on the specific goals of a unit or organization. If the immediate requirement is unity and trust, loyalty becomes indispensable. If, however, the primary objective is to achieve rapid effectiveness in highly technical or complex operations, then professionalism and expertise may take precedence. At the same time, servicepersons acknowledge the difficulty of working with individuals who are highly professional but not loyal, as their actions may run counter to the organization's core interests or values. This is a dilemma in which the details are important. While loyalty to the mission is indispensable, professional competence is valuable. Lack of either is fraught with dire consequences. Meanwhile, shifts in the political situation and different visions regarding the best leadership style, as well as various other factors, may have an impact on the professional's loyalty, which in different circumstances may be displayed in a different way. Quite often this dilemma may be resolved by simply moving the professional away from an uncomfortable situation to a position where they may safely exercise their duty without loyalty needing to play such an important part.

Born vs trained leaders

A common thought is that some individuals are born leaders, where emphasis is placed on their personal traits and natural talent. Advocates for the trained leader, however, argue that leadership is not innate, but rather that anyone can learn to become a good leader.

Which category individuals fall into often depends on cultural heritage, values, and experience. For example, the experience in Croatia shows that talent certainly helps, as born leaders have found it easier to motivate and inspire others. At the same time, education and training are indispensable, particularly in the context of modern warfare, where technological complexity and rapid decision-making require preparation and adaptability.

In reality, both aspects are important. Talent provides a natural advantage, but training ensures consistency, professionalism, and readiness for today's challenges. Modern times therefore call for a new approach to education and training, one that combines personal development with structured preparation.

Ultimately, to serve well as a leader, one must live by principles, values, and commitment. The foundation of effective leadership lies in investing in your people – nurturing their potential, supporting their growth, and building trust.[20]

The Ukrainian experience since the beginning of the war provides a compelling case study. Many civilians with little or no prior military background have stepped into leadership positions almost overnight. Through accelerated training and real-life experience, they have adapted to new responsibilities, proving that leadership potential can emerge even without years of preparation. Compared with the pre-war period, leaders in the Armed Forces of Ukraine are significantly younger and are often distinguished by notable military achievements, their ability to adapt quickly, and a freedom from Soviet-era hierarchical attitudes that once constrained innovation and initiative. This generational shift has reshaped leadership culture, prioritizing initiative, adaptability, and responsibility over rigid formality. Ethical and adaptive leadership is cultivated through character as well as deliberate investment in education and mentorship.

20 Defence ethics training, Ukraine, August 2025.

The role of NCOs in leadership

The role of NCOs in shaping leadership structures and safeguarding ethical values cannot be underestimated. Traditionally, NCOs have been the backbone of military organizations worldwide, serving as the bridge between enlisted personnel and officers. Crucially, NCOs also function as the primary custodians of ethical conduct within units. Through daily interaction with soldiers, they model professional behaviour, address misconduct early, and ensure that ethical standards are upheld even under pressure. By reinforcing norms of integrity, accountability, and respect, NCOs help create a command climate in which soldiers understand both what is expected of them and why ethical discipline matters. Their leadership contributes to resilient values-based organizations where responsibility and initiative are distributed across all levels.

Example: The role of NCOs in Ukraine

In Ukraine, the importance of training NCOs has steadily grown, evolving from a rigid and highly hierarchical Soviet system into a decentralised structure aligned with NATO standards. The Soviet NCO training model focused on ideological loyalty and technical skills, with the Praporshchik (warrant officer) rank system forming a separate career track between enlisted personnel and commissioned officers.[21]

The 2014 Russian aggression accelerated reforms to develop professional NCOs and not mere order-followers, enhancing their combat capabilities and granting them greater decision-making authority and leadership responsibilities. NCO training was modernized with NATO-aligned curricula, new educational centres, simulators, and joint exercises with international partners.[22]

The 2019 law № 205-IX reformed the sergeant ranks, abolishing the former Soviet-style Praporshchik titles and introducing staff sergeant (battalion level), master sergeant (brigade level), senior master sergeant (operational, air, marine command level), and chief master sergeant (senior NCO level), thereby increasing their authority and responsibilities.[23] In 2022, the Concept of development of the Professional NCO Corps of the Armed Forces of Ukraine set a roadmap until 2035, emphasizing leadership development and strengthening the armed forces' combat effectiveness.[24]

During the full-scales Russian invasion, NCOs have played a crucial role in defence, often serving as platoon and company commanders and directly leading front-line operations due to shortages of commissioned officers or their limited practical experience. As Chief Sergeant of the Armed Forces of Ukraine, Oleksandr Kosynskyi stated, 'War is not about education; it is about abilities, training, and experience.' Off the battlefield, NCOs fulfil a crucial role in force generation by training new recruits in role-specific skills tailored to operational conditions.[25]

As a testament to the NCOs' crucial role in guaranteeing operational success, since 2014, over 25,000 NCOs have been recognized with state awards, including 105 Heroes of Ukraine, 76 of which have been awarded posthumously.[26]

---

21 Р. Кузьменко, "Підготовка сержантського складу в умовах сучасної війни: виклики та перспективи," *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського* (23 January 2025): 100–103, https://doi.org/10.33099/2304-2745/2024-3-82/100-103

22 Ibid.

23 Армія FM, "Реформування Сержантського Корпусу," Армія FM, 11 December 2019, https://www.armyfm.com.ua/reformuvannya-serzhantskogo-korpusu/

24 Євген Проворний, "Набула чинності нова 'Концепція розвитку професійного сержантського корпусу ЗСУ,'" Armyinform.com.ua, 22 November 2024, https://armyinform.com.ua/2022/12/21/nabula-chynnosti-nova-konczepcziya-rozvytku-profesijnogo-serzhantskogo-korpusu-zsu/

25 Євген Проворний, "День сержанта ЗСУ: про військове мистецтво, відмову від офіцерських посад та про удостоєних звання Героя України," Armyinform.com.ua, 3 September 2025, https://armyinform.com.ua/2024/11/18/den-serzhanta-zsu-pro-vijskove-mystecztvo-vidmovu-vid-oficzerskyh-posad-ta-udostoyenyh-zvannya-geroya-ukrayiny/

26 Ibid.

NATO countries agree that sergeant training is now fully synchronized with officer training, ensuring that NCOs have a comprehensive understanding of operational dynamics. This means that sergeants are no longer confined to narrow, tactical responsibilities but are equipped to see the broader picture and contribute to decision-making at higher levels. Sergeants are increasingly seen as operational commanders, with the Chief Sergeant of the Armed Forces of Ukraine standing as a prominent example of the authority and influence that NCOs can wield. Given the intensity of the war, Ukraine does not have the luxury of experimenting with entirely new systems or overhauling structures from scratch. Instead, the focus is pragmatic: identify individuals who display leadership potential, give them opportunities to grow, and allow them to take command when needed. This pragmatic approach has already borne fruit, as many officers and NCOs who faced the earliest and most critical stages of Russian aggression have since risen into key leadership positions, bringing with them invaluable front-line experience, ethical decision-making, and credibility.

Underlying the discussion on this topic during defence ethics training in Ukraine in August 2025 was a broader understanding of leadership as more than the actions of a single individual. True leadership, participants stressed, involves the continuous development of a self-sufficient organization where responsibility is shared and succession is natural. A well-functioning unit should not collapse if its commander is absent; instead, subordinates should be prepared and empowered to assume leadership seamlessly. This approach builds resilience and continuity. It also reinforces the principle that leadership is not static; it evolves with circumstances, challenges, and the development of those within the organization. By fostering an environment where initiative and accountability are valued at every level, from junior sergeants to senior officers, the Armed Forces of Ukraine are cultivating a new model of leadership suited to the realities of modern warfare.

Remember that

- Leadership is service — integrity and dignity build trust.
- Ethical leaders balance confidence, humility, empathy, and accountability.
- Leaders must resolve dilemmas — loyalty vs professionalism, talent vs training.
- Future warfare demands rapid, ethical decision-making — train and prepare.
- NCOs safeguard ethics daily through example and enforcement.
- Civilian and military leadership roles complement each other.
- Meritocracy matters — develop people and promote based on character and ability.

Check-your-skills exercises

Task 1. Loyalty oath and ethical principles

Activity description (for participants):

Read the *Loyalty Oath for Military Personnel of the Republic of Georgia* (25 May 2024). Reflect on its meaning and identify the ethical principles embedded in the text. Discuss which parts of the oath are primarily legal obligations, which are ethical commitments, and where they overlap.

[Loyalty oath] for military personnel of the Republic of Georgia:

'I, (name), born on (date) in (location), a citizen of Georgia, do swear before the Holy Trinity and my country to honestly and faithfully serve the people of Georgia, protect the independence and territorial integrity of my homeland, and fulfil my military duties and the orders of my commanders. I pledge to keep military and state secrets, uphold the constitution and laws of Georgia, and defend the principles of democracy and human rights. I swear to never betray my country or the trust placed in me as a soldier. Should I break this oath, I am prepared to bear the full responsibility and accept the consequences of my actions as determined by the laws of Georgia. So help me God.' (25 May 2024)

Guiding questions:

1. Which of the following elements express ethical principles? What does each principle mean in practice?
   - Honestly and faithfully serve the people (my fellow citizens)
   - Protect the independence and territorial integrity of the nation
   - Fulfil my military duties
   - Obey orders of my commanders
   - Protect, and do not reveal, military and state secrets
   - Uphold the constitution
   - Uphold the laws
   - Defend the principles of democracy and human rights
2. Beyond what is written in the oath, what additional character traits are essential for leaders to be able to command effectively?
   - Honesty
   - Fairness (impartiality)
   - Integrity (strength of character)
   - Moral courage (courage to act ethically under pressure)
   - Trustworthiness
   - Incorruptibility
   - Others (e.g. humility, empathy, resilience)

Facilitator notes:

- Highlight the difference between legal duty (e.g. upholding the constitution, protecting state secrets) and ethical duty (e.g. honesty, fairness, courage).
- Draw comparisons with other countries' oaths or codes of ethics to broaden perspective.
- Stress that oaths are more than symbolic – they set a standard for ethical conduct and public trust.

Task 2. Case discussion: Supervising an errant soldier

Activity description (for participants):

Read the case study carefully. The scenario presents a leadership dilemma: balancing fairness, discipline, and compassion. Discuss possible courses of action and their implications for the individual soldier, the unit, and the leader's credibility.

Case summary:

'A specialist in my company came into my office one morning after going on sick call. The soldier had a reputation in the command for being a hard worker and doing his job well. When he came to me with a quarters slip from sick call, which stated he had the flu, I did not question it and signed the quarters slip recommending the soldier for 24-hour quarters. As I drove home that evening, I passed a bar and thought I saw the soldier's car in the car park. My first sergeant (1SG) went to the nightclub and found the soldier there. When the 1SG confronted the solider, he claimed he did not know that being "on quarters" meant he was required to stay at home or, in his case, the barracks. I didn't want to "slam" a good soldier, but what will other soldiers do if I don't address this issue?'

Guiding questions:

1. What values and ethical principles are at stake in this case (trust, fairness, discipline, accountability, integrity)?
2. What are the possible options for the commander?
   - Ignore the incident (show leniency).
   - Apply disciplinary action strictly (enforce rules).
   - Apply corrective but measured action (balance fairness and discipline).
3. What are the risks of being too lenient? What are the risks of being too harsh?
4. How will the decision affect unit morale, discipline, and trust in leadership?
5. What lesson should the soldier – and the rest of the unit – take from the decision?

Facilitator notes:

- Push participants to consider long-term consequences of leadership decisions, not just immediate outcomes.
- Explore the role of moral courage: making a fair decision even if it is unpopular.
- Ask participants to think about consistency: What precedent does the leader set for future cases?
- Highlight that discipline is not about punishment for its own sake, but about maintaining trust, fairness, and unit cohesion.
- Encourage reflection: How would participants want their own leader to handle such a situation?

03

Key ethical dilemmas in the defence sector

The routine operation of military organizations frequently presents a variety of opportunities for “going off the rails,” forgetting the service’s core values, ignoring its regulations, or even succumbing to the kinds of organizational social conditioning described above that may lead even good people to do bad things. There are indeed many opportunities for “things to go wrong.” In this module, we will examine some of the most familiar and potentially treacherous pitfalls that military organizations and their personnel are likely to confront. Even when a military force is not actively engaged in armed conflict with enemies and adversaries and defending the nation it serves and protects, for example, the individual members of the organization will be involved in a variety of tasks and activities that must be carried out in order to support and prepare the organization to fulfil its primary function. Recruiting and training a continuing supply of new soldiers, sailors, or marines is a fundamental requirement to build and sustain the military’s ability to carry out its duty of national self-defence. Securing equipment and supplies necessary to sustain the organization in carrying out that duty: weapons and armaments, for example, food and medicine, transportation and housing for troops and their families. Senior military leaders must organize, govern, and train their junior personnel, ensuring that the entire force is prepared to engage in combat if necessary. The resulting “chain of command” affords a great deal of power, authority, and discretion to those of higher rank and experience to carry out these duties. Power and authority, however, can be exercised irresponsibly, and even abused.

There are, in short, ample opportunities for unethical behaviour and professional misconduct even under the most routine circumstances. Some of the more common pitfalls will be examined and discussed in this section.

3.1. Mistreatment and discrimination

We who wear the cloth of our nation understand that cohesion is a force multiplier. Divisiveness leads to defeat. As one of our famous presidents said, 'A house divided does not stand.'

– General Mark A. Milley, Chairman of the Joint Chiefs of Staff (2020)

Module objectives

To understand the forms, consequences, and ethical implications of mistreatment and discrimination within defence institutions; to recognize how such conduct undermines professionalism, operational effectiveness, and human dignity; and to identify strategies to prevent, respond to, and redress such practices through ethical leadership and institutional accountability.

Key information

- Discrimination and mistreatment are common ethical challenges in military organizations, often manifesting through abuse of power, unequal treatment, or harassment.
- Such conduct violates basic human rights, erodes morale and cohesion, and undermines operational readiness, efficiency, and public trust.
- Mistreatment may be psychological, physical, or structural – that is, embedded in institutional systems, policies, or cultures – and includes both individual acts and systemic practices.
- Discrimination undermines fairness by targeting individuals based on irrelevant traits such as race, gender, religion, sexual orientation, ethnicity, or other, rather than their abilities or contributions.
- Addressing mistreatment and discrimination requires individual integrity, committed leadership that fosters a culture of respect, and robust institutional mechanisms of oversight, reporting, and accountability.

Module content

Definitions

Discrimination is commonly understood as the unfair treatment of individuals or groups based on irrelevant characteristics such as race, gender, religion, ethnic identity, sexual orientation, or disability. Stereotypes are generalized beliefs about certain groups; prejudice is a biased attitude towards them; and discrimination is the *behavioural* expression of those beliefs or attitudes – *actions or decisions* that deny equal opportunities.

- **Direct discrimination:** Explicitly treating someone less favourably because of a protected characteristic (e.g. refusing to promote a qualified soldier because she is a woman)
- **Indirect discrimination:** Policies or practices that appear neutral but disadvantage certain groups (e.g. physical test standards unrelated to job performance that disproportionately exclude certain groups).

Example: Wearing a beard while serving in the British military

For decades, the British Armed Forces enforced strict grooming standards that effectively banned beards except in limited circumstances such as medical or religious necessity. In practice, these exemptions were tightly controlled and did not always capture the broader cultural or identity-based importance of beards. For many Muslim, Sikh, or other religiously affiliated personnel, wearing a beard is not only a matter of religious obligation but also a cultural marker of belonging and identity. The persistence of a clean-shaven ideal within the forces meant that service members who wore beards could face stigma or pressure to conform, even when technically exempt. After years of advocacy and internal review, policy changes unfolded: the Royal Air Force formally started to permit beards in September 2019; the British Army lifted its beard ban in March 2024, introducing strict guidelines (e.g. beard length limited to 2.5–25.5 mm, neat and full beard only)[27]; the Royal Marines have maintained their clean-shaven tradition, although internal discussions on reform continue. These reforms reflect a broader shift towards inclusion, acknowledging that seemingly neutral grooming rules can produce unequal outcomes when applied without accommodation.[28]

Mistreatment refers to harmful interpersonal behaviours that cause physical or psychological harm to an individual, regardless of group identity or protected status. It encompasses actions that degrade, intimidate, or isolate others, such as:

- **Personal harassment:** Bullying, insults, intimidation, spreading of rumours, or repeated offensive remarks.
- **Sexual harassment:** Unwanted sexual advances, suggestive comments, or physical contact.
- **Physical harassment:** Physical violence or threats thereof.

While discrimination often results in tangible career consequences – such as unequal pay, promotions, or assignments – mistreatment primarily undermines psychological safety and workplace culture, which can, beyond creating a hostile environment, have serious operational consequences by eroding trust, cohesion, and morale.

27 Veronika Melkozerova, 'British Army Lifts Century-Old Beard Ban', POLITICO (29 March 2024), https://www.politico.eu/article/british-army-lifts-100-year-old-beard-ban-for-soldiers-and-officers

28 Julian Perreira, 'Senior Royal Marines Officials Reviewing Ban on Beards That Could Soon Be Scrapped', bfbs Forces News (13 January 2025), https://www.forcesnews.com/services/royal-marines/senior-royal-marine-officials-are-reviewing-ban-growing-facial-hair-and

Mistreatment and discrimination in the defence sector have consequences that ripple beyond individual victims, affecting the institutional structures and overall operational capability of the armed forces. These impacts can be considered at three interconnected levels – individual, where personal well-being, trust, and career prospects are harmed; structural, where institutional norms and hierarchies perpetuate or intensify toxic cultures and unequal treatment; and the organizational level, where these dynamics collectively undermine cohesion, effectiveness, and public confidence in the armed forces. See Fig. 3.

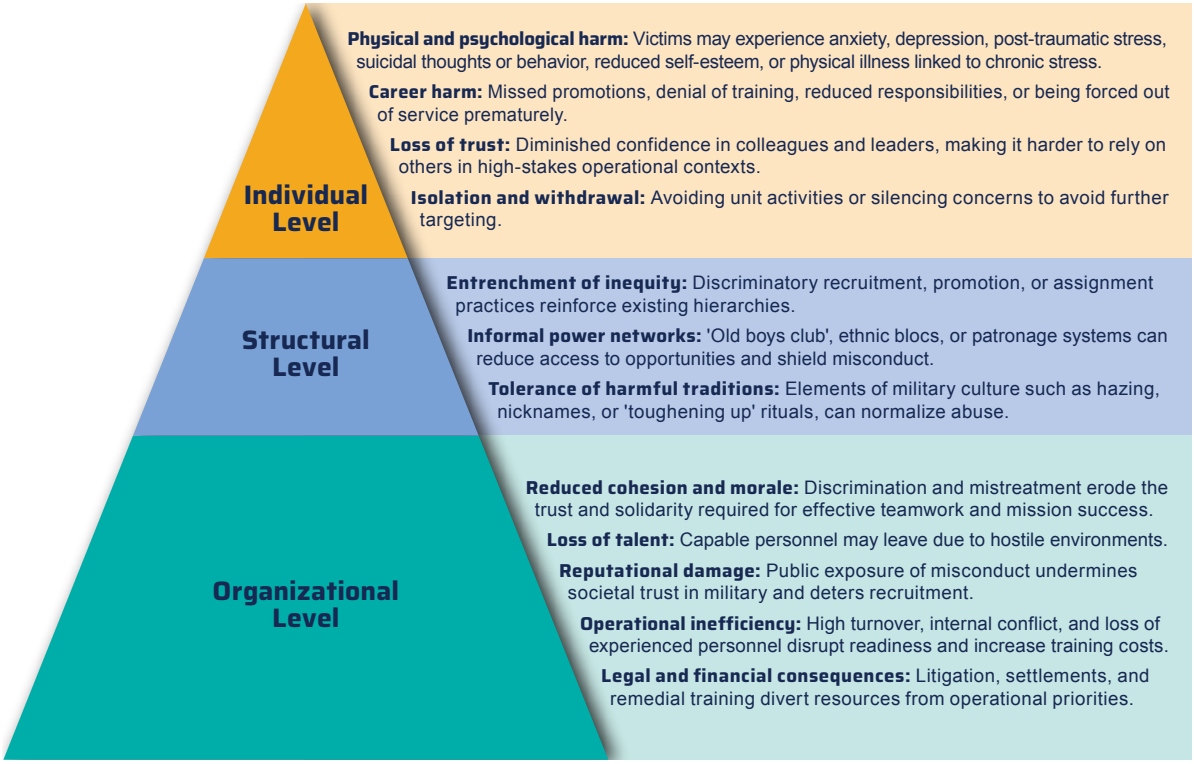

Figure 3. Interconnected levels of impact of mistreatment and discrimination in the defence sector

Ethical dilemmas in mistreatment and discrimination

While most forms of discrimination and mistreatment in the military are clearly prohibited under law and conduct codes, genuine ethical dilemmas arise when operational requirements and the protection of individual rights and dignity come into conflict. Leaders bear particular responsibility for navigating these situations, where maintaining discipline, loyalty, and cohesion can conflict with confronting harmful behaviour or challenging entrenched cultural norms. Such dilemmas often emerge in contexts where silence is justified as loyalty, hardship blurs into abuse, or tradition is used to excuse mistreatment. Addressing them requires leaders to reconcile mission demands with the imperative to safeguard individual rights, uphold respect and fairness, and preserve the moral credibility of the institution.

When does operational necessity turn into discrimination?

Operational requirements sometimes demand selection based on religion, language, cultural knowledge, or even diet. For example, assigning personnel fluent in the local language to intelligence roles may be necessary for mission success. However, when such criteria exclude capable candidates without clear necessity – such as excluding women from front-line service due to perceived risks – the line between justified operational planning and unlawful discrimination becomes obscured. The ethical challenge lies in applying operational criteria narrowly, ensuring they are proportionate to mission needs and are based on clear evidence-backed necessity rather than on convenience or stereotype.

Example: Women in combat roles

Throughout much of modern military history, women were formally excluded from close combat roles in both the US and the UK. Justification for these exclusions centred on assumptions about unit cohesion, physical capacity, and emotional resilience. Yet the operational experience of Iraq and Afghanistan partly challenged these claims. In conflicts without clear front lines, women in support roles – such as medics, engineers, and the military police – routinely faced combat conditions and performed effectively alongside male colleagues. Their real-world performance undermined the notion that gender determined combat effectiveness and revealed that exclusionary policies rested on untested assumptions rather than evidence. Recognizing this, the US lifted its ban on women in combat in 2013. The UK followed suit in 2016, marking a shift from assumption-based exclusion to evidence-based policy grounded in individual capability and operational performance.

Example: Female soldiers in Ukraine

The full-scale invasion of 2022 accelerated the integration of women into Ukraine's armed forces, with more than 47,000 serving by early 2024, including over 5,000 on the front line. Initially, women faced systemic barriers: uniforms, footwear, and body armour were designed for men, forcing servicewomen to alter clothing at their own expense or rely on volunteers. Civil society initiatives such as ArmWomenNow and Zemlyachky helped expose this institutional gap by developing and distributing women's uniforms, underwear, and body armour based on NATO standards.[29] Their prototypes underwent testing by the Ministry of Defence in 2022–23, leading to a structural reform of the procurement system. By 2023, women's summer field uniforms and underwear were formally included in the centralized supply, and in 2024, 65,000 sets were issued – meeting the needs of all servicewomen. That same year, the ministry approved the first two models of women's body armour, tested under combat conditions.[30]

This reform represented an ethical and operational turning point: the institution shifted from expecting women to adapt to ill-fitting male equipment to adapting its own systems to the realities of a gender-diverse force. By addressing long-standing neglect, Ukraine's Ministry of Defence strengthened not only safety and combat readiness but also institutional legitimacy, signalling that equality and inclusion are integral to effectiveness in modern warfare.

Can military traditions excuse mistreatment or abuse?

Military traditions are often designed to foster cohesion, discipline, and resilience through shared rituals such as assigning nicknames, initiating newcomers, or testing endurance. Yet ethical tension arises when the preservation of tradition conflicts with the duty to uphold human dignity, respect, and lawful conduct. When such practices involve humiliation, coercion, discrimination, or physical harm, they cease to be legitimate tools of cohesion and become forms of mistreatment or abuse.

29 'За Стандартами НАТО: Як Організація ArmWomenNow Створює Жіночу Військову Форму', 23 July 2023, https://www.ukrinform.ua/rubric-society/3739238-za-standartami-nato-ak-organizacia-armwomennow-stvorue-zinocu-vijskovu-formu.html; Українська Правда. Життя. 'Волонтери Запускають Пошив Військової Жіночої Форми з Урахуванням Особливостей Фізіології. ФОТО'. Accessed 29 August 2025. https://life.pravda.com.ua/society/2022/10/28/251046/

30 '(Не)Рівність у Строю: Дослідження Рівня Забезпечення Військовослужбовиць ЗСУ'. *State Watch*, 12 October 2024, https://statewatch.org.ua/publications/ne-rivnist-u-stroiu-doslidzhennia-rivnia-zabezpechennia-viyskovosluzhbovyts-zsu-vidpovidnym-boyovym-komplektom/

These issues are not isolated acts of misconduct but symptoms of deeper institutional culture and oversight failures, where harmful behaviour is tolerated or justified as 'tradition'. Leaders bear responsibility for recognizing and addressing these practices, ensuring that cohesion is built on trust and mutual respect, not fear or exclusion.

Ultimately, tradition cannot be used to justify unlawful or dehumanizing conduct. Cohesion achieved at the expense of dignity undermines the very values of professionalism, integrity, and mutual respect that military institutions claim to uphold.

Example: Parris Island hazing scandal

In 2017, a former US Marine Corps drill instructor at Parris Island, South Carolina, was convicted of abusing and assaulting recruits in what he claimed were traditional methods of discipline. His actions included tumbling a Muslim recruit in an industrial clothes dryer, forcing recruits to choke one another, making them drink excessive amounts of chocolate milk until they vomited, and walking on top of them while they lay crammed into a room.

The investigation that led to his court-martial was sparked by the March 2016 death of 20-year-old recruit Raheel Siddiqui, who fell from a barracks balcony after what official reports described as an 'altercation' with the same instructor. Siddiqui's death prompted a broader inquiry into Parris Island's training culture, revealing patterns of hazing, verbal and physical abuse, and targeted mistreatment – particularly against recruits from minority backgrounds.

While some senior NCOs defended certain practices as part of the 'toughening up' process essential to Marine training, the investigation concluded that these acts crossed the line into unlawful abuse. The case triggered widespread reforms in recruit training oversight, instructor supervision, and hazing prevention policies.

When does military hardship become abuse?

Military life inevitably involves discomfort and stress. International human rights law recognizes that some acts which might be considered degrading in civilian life may be permissible within the armed forces if they serve a legitimate training purpose, contribute to operational readiness, and remain within the 'unavoidable level of hardship inherent in military discipline'.[31] The central ethical and legal dilemmas arise when survival training, simulated captivity, or physically extreme drills are pushed beyond what is justifiable harm necessary for preparation. Training practices cross that line when they exceed the requirements of operational preparation, disregard health safeguards, or compromise the dignity and safety of personnel.

Whether hardship remains legitimate depends on intent, proportionality, informed consent, medical oversight, and respect for human dignity. When these safeguards are ignored, training risks becoming a form of inhuman or degrading treatment rather than lawful discipline.

31 Council of Europe. Committee of Ministers. *Recommendation CM/Rec(2010)4 on the human rights of members of the armed forces: Explanatory Memorandum*. CDDH – Steering Committee for Human Rights, 1077th meeting, Strasbourg, 2010. Available at: https://search.coe.int/cm?i=09125948801e76bd; see also European Court of Human Rights. Case of Chember v. Russia (7188/03), 01/12/2008. Available at: http://hudoc.echr.coe.int/eng?i=001-87354, para. 49.

Example: Selection for special forces

One of the most demanding military selection processes includes a stage known informally as an intense multi-day endurance event, during which candidates undergo continuous physical exertion, exposure to harsh environmental conditions, and extreme sleep deprivation. In one recent year, a candidate died shortly after completing this phase, prompting an official investigation into the programme's safety and oversight mechanisms.

The subsequent review identified significant systemic failures, including insufficient medical supervision, a training culture that normalized serious health risks, and institutional resistance to change despite prior warnings. Investigators also noted that in the years leading up to the incident, aspects of the course had been intentionally intensified in response to criticisms that standards were becoming too permissive – reinforcing a mentality that equated resilience with withstanding avoidable harm and diminishing the duty of care owed to candidates.

In the aftermath, authorities introduced a series of reforms, such as continuous medical monitoring, restrictions on high-risk practices, and stronger controls on performance-enhancing substances. Nevertheless, the case exposed wider shortcomings in organizational oversight and leadership accountability, demonstrating how entrenched cultural norms can create conditions where foreseeable harm is allowed to persist under the guise of tradition or toughness.

Ultimately, the legitimacy of military hardship depends not only on its contribution to mission readiness but also on adherence to legal and ethical standards that safeguard health, consent, and dignity. Conditioning that disregards these principles ceases to build strength; it erodes trust, undermines morale, and damages the moral authority of the institution itself.

Does loyalty justify staying silent about mistreatment in the field?

During operations, the chain of command and mutual trust are essential for cohesion and mission success. Yet these same principles can create profound ethical tension when misconduct occurs within the ranks. The core dilemma lies in the conflict between preserving immediate operational cohesion and fulfilling the long-term obligation to uphold legal and ethical standards. Reporting a superior or comrade for abusive or discriminatory conduct can be perceived as betrayal, threatening unity or morale in the field. Such perceptions form powerful barriers to reporting, especially in close-knit units where loyalty is prized above all else.

However, silence in such circumstances is not neutral – it amounts to active complicity, enabling further harm and allowing a culture of abuse to take root. When wrongdoing goes unreported, it endangers individuals, corrodes trust, and undermines the moral authority of the entire chain of command. True loyalty cannot mean protecting misconduct; it must mean protecting the integrity of those who serve.

Example: Culture of violence and mistreatment during deployment

An independent military inquiry released its findings on serious misconduct within a special operations community during overseas deployments spanning more than a decade. The investigation uncovered credible evidence of dozens of unlawful killings and other grave violations of international humanitarian standards. The consequences were extensive: criminal referrals, the withdrawal of collective honours, and wide-ranging organizational reforms. Notably, the inquiry concluded that these acts did not arise from the pressures of combat but from an internalized subculture characterized by distorted notions of loyalty, honour, and elite identity. Certain initiation practices – including forcing junior personnel to participate in unlawful violence – were used to demonstrate allegiance and toughness, reinforcing internal cohesion while dehumanizing detainees.

The inquiry also revealed a pervasive culture of silence. Many witnesses acknowledged that they had not reported abuse due to fear of ostracism, retaliation, or damage to their careers. This silence was found to reflect systemic failures in leadership, oversight, and the absence of effective whistle-blower protections, which collectively enabled misconduct to continue across multiple rotations.

In response, authorities initiated disciplinary action, revoked honours for implicated units, and committed to reforms in training, leadership development, and accountability systems. However, the case continues to raise questions about whether structural reforms alone are sufficient to address the deep-seated cultural dynamics that permit silence, complicity, and the normalization of unethical behaviour.

Ultimately, professional military ethics demand courage not only in combat but also in confronting wrongdoing, even when doing so risks short-term disruption to unity. Upholding law, human dignity, and institutional integrity is the highest form of loyalty – to one's comrades, one's profession, and the mission itself.

Good practice or solution?

Addressing mistreatment and discrimination in the defence sector requires both a strong ethical culture and robust institutional safeguards. Leaders and personnel alike face what can be called a **test of integrity** – a situation where the correct course of action is clear in principle but difficult in practice due to pressures that discourage ethical action – e.g. peer pressure, loyalty, or fear of reprisal. Addressing mistreatment and discrimination in the defence sector requires a combination of preventative, protective, and accountability measures. The following elements are essential to creating an environment where dignity and respect are upheld:

- **Clear definitions and standards** in military codes of conduct that leave no ambiguity about what constitutes mistreatment or discrimination
- **Active bystander training** so all personnel know how to intervene or report without compromising safety
- **Multiple reporting channels**, including confidential options outside the immediate chain of command
- **Accountability at all levels**, ensuring leaders are responsible for the environment in their units
- **Independent oversight bodies** empowered to investigate and act on complaints, reducing fear of bias or retaliation
- **Targeted evidence-based initiatives** to dismantle harmful norms and normalized abuse, supported by clear indicators of progress and strong role-modelling from senior personnel.

Taken together, these measures form an integrated set of principles that reinforce one another in building an ethical and accountable environment. Clear standards are meaningful only when paired with genuine accountability; reporting mechanisms are effective only when personnel are trained and empowered to use them safely; and structural reforms need the support of independent oversight and sustained cultural change to ensure they take root. Their interdependence is what ultimately ensures that dignity and respect are not just stated values but lived realities within the institution.

Any tendency to treat one's own situation as an exception to these standards – whether due to operational urgency, tradition, or loyalty – is a warning sign of failing the test of integrity. In those moments, the duty to uphold human dignity, lawful conduct, and professional standards must take precedence over personal comfort, group acceptance, or institutional convenience. Ultimately, ethical standards are non-negotiable, even under operational pressure, and compromising them not only harms individuals but also undermines mission effectiveness and weakens institutional legitimacy.

Remember that

- Mistreatment and discrimination are not minor misconduct – they undermine dignity, cohesion, and operational effectiveness.
- Discrimination can be direct or indirect – neutrality in rules does not guarantee fairness in outcomes.
- Tradition and operational necessity never justify abuse or dehumanization.
- Military hardship is legitimate only when necessary, proportionate, and respectful of human dignity.
- Silence in the face of mistreatment is not loyalty – it enables harm and erodes institutional integrity.
- Ethical leadership requires the courage to challenge harmful norms, even under operational pressure.
- Prevention, reporting and accountability mechanisms are effective only when leaders actively uphold and model them.

Check-your-skills exercises

Task 1. 'Mistreatment or discrimination? Identifying impact and responses'

Objective:

- To help participants recognize different forms of mistreatment and discrimination
- To analyse different implications that mistreatment and discrimination have on individual, structural and organizational levels
- To critically reflect on causes of and contributing factors to mistreatment and discrimination in the defence sector
- To explore strategies to address mistreatment and discrimination.

Duration: 50–60 minutes

Group size: 10–25 participants (3-6 per group)

Materials needed:

- Scenario handouts
- Pens

Instructions:

1. Introduction (5 minutes):

The instructor briefly introduces the activity: 'Discrimination and mistreatment often appear in subtle or normalized ways. In this exercise, you'll work in small groups to analyse four different types of scenario. The task is not just to identify whether behaviour is acceptable, but to consider its wider consequences and how it should be addressed.'

2. Group work (20–25 minutes):

Each group receives one scenario and discusses the following questions:

- Can the situation described in this scenario be considered mistreatment or discrimination? Why or why not?
- What are the causes and factors contributing to mistreatment or discrimination in this scenario?
- What are the individual, structural, and organizational implications of this scenario – for the person(s) directly involved, for the way the unit operates, and for the wider institution?
- How could this issue best be addressed at each of these levels – individual, structural, and organizational – to prevent harm and strengthen professionalism?

01

Scenario 1: PPE and Deployment

A mixed-gender unit is preparing for deployment. The commander is informed that only about 20% of the required personal protective equipment (PPE) in women's sizes has been delivered. Rather than escalating the issue or seeking solutions, he decides to reassign all female soldiers to lower-risk tasks until the shortage is resolved.

02

Scenario 2: The Inner Circle

After formal briefings, a commander regularly invites a small group of soldiers (all white male NCOs) to stay behind for 'informal chats' or to social events such as barbecues. Over time, these same individuals consistently receive the best assignments and faster promotions compared with their peers.

03

Scenario 3: Squad Nicknames

Within a platoon, members use nicknames for each other. Some are harmless or even affectionate, but others are based on stereotypes or personal traits, for example, calling a female colleague 'princess', referring to a smaller soldier as 'shorty', or labelling a soldier from a Turkish background 'the Turk'. Most soldiers dismiss this as 'tradition' or 'banter', but a few feel humiliated and excluded.

04

Scenario 4: Training Punishment

During a field exercise, an instructor punishes late arrivals by forcing them to repeatedly crawl through mud under barbed wire, continue running drills with full gear despite dehydration, and perform push-ups until collapsing. Several recruits show signs of heat exhaustion, but the instructor insists that 'only the toughest will make it' and that such punishments are essential for building resilience.

Figure 4. Details of the scenario handouts

3. Plenary discussion (25–30 minutes):

Groups present their findings to the plenary (5 minutes each). After each presentation, the instructor facilitates discussion by drawing out key learning points, such as:

- Understanding that mistreatment and discrimination can take different forms and are not always obvious at first glance
- Recognizing that there does not necessarily need to be bad intent behind harmful practices; they may arise from tradition, convenience, or structural gaps rather than deliberate malice
- Considering the ripple effects of individual incidents on morale, cohesion, and operational effectiveness
- Exploring the complexity of leadership decisions where operational requirements and ethical standards intersect
- Identifying practical strategies for prevention, reporting, and accountability at multiple levels.

Expected outcomes:

- Enhanced ability to differentiate between mistreatment and discrimination.
- Recognition of causes and factors contributing to mistreatment and discrimination.
- Recognition of impacts at multiple levels: personal harm, systemic bias, and organizational culture.
- Practical reflection on interventions at leadership, policy, and peer levels.
- Increased awareness that normalized practices can undermine cohesion and integrity.
- Foundation for further modules on professionalism and abuse of power.

3.2. Nepotism in the defence sector

Module objectives

To understand the concept, historical background, and various forms of nepotism – particularly in defence institutions – and to critically evaluate its ethical, legal, and organizational implications, enabling the participants to recognize it as a violation of professional integrity and to uphold standards of impartiality and accountability in decision-making.

Key information

a. Nepotism is the preferential treatment of family or close associates in appointments or promotions, often regardless of merit. The term originates from the Latin *nepos* (nephew).

b. Nepotism remains widespread, even in modern democracies.

c. In military settings, nepotism can lead to:

- Promotions of unqualified individuals
- Erosion of morale, integrity, and public trust
- Creation of artificial posts to benefit relatives. These practices compromise operational efficiency, violate military ethics codes, and waste resources.

d. While nepotism is often illegal or prohibited by codes of conduct, enforcement varies. Many countries recognize it as a form of political corruption. Institutions such as Transparency International use nepotism as a corruption indicator.

e. Although generally harmful, nepotism may be seen in post-conflict or conflict environments where loyalty and trust are critical (e.g. during war or in fragile states). In some cultures, familial recruitment reflects tradition rather than corruption.

f. Engaging in nepotism is a 'test of integrity', not a moral dilemma. Leaders must uphold professional and legal standards over personal loyalty. Refusing to favour family is a core demonstration of public service ethics.

Module content

Nepotism consists of favouritism shown, or special treatment accorded, to members of an individual's immediate or extended family or circle of friends.

The word **nepotism** is derived from the Latin *nepos* (nephew) and stems from the medieval practice of popes and bishops (who had no legitimate children of their own) appointing their nephews to positions of high power and trust in the Catholic Church. Some of the powerful Borgia family in Italy, after themselves having been chosen as pontiff, managed to have many of their male relatives appointed as cardinals, and thus ready to ascend to the papacy themselves following the death of their benefactor. But the practice antedates Christianity, and seems to constitute a form of feudalism, filial piety, or family loyalty widely practised in many cultures.

In modern times, the practice is just as widespread in the military as it is in politics and government, financial institutions, and other business and commercial organizations.[32]

While toleration of the practice varies widely in different countries and services, the opportunities and temptations to engage in the practice are near universal. Examples in the military would include a recruitment officer influencing the screening and application process to benefit a friend or family member, even one less qualified than other applicants. A senior officer might intervene in or tamper with the normally impartial staff hiring process to obtain a lucrative civilian support job for a spouse, child, or relative. Perhaps the most egregious form of the practice would be interfering in official promotion selection boards to ensure that a close friend or family member receives inappropriate special consideration for promotion to a higher rank.

Interesting fact: In Georgia, those who are allegedly recruited through methods linked to nepotism are called 'flowerpot'.

Definitions

Nepotism refers to preferential treatment of family members, often by placing them in military positions, awarding them promotions, or facilitating recruitment, regardless of merit or qualifications. *Example: A senior officer arranging for their daughter to be promoted ahead of more qualified candidates.*

Favouritism is a broader term that refers to unfair preferential treatment of individuals based on personal preference, friendship, or emotional bias rather than on objective performance or merit. *Example: A unit commander consistently assigning favourable duties to a conscript they personally like, despite poor performance.*

Cronyism is the appointment or promotion of friends and close associates – especially in leadership or advisory roles – based on loyalty or personal relationships rather than competence or experience. *Example: Selecting a close personal friend to lead a procurement unit despite lack of relevant expertise.*

See Table 2, which sets out the differences between nepotism, favouritism, and cronyism. Needless to say, all three of these undermine merit-based decision-making and institutional integrity and lead to reduced morale, resentment, and loss of public trust. Furthermore, they contribute to operational inefficiency and lowered professional standards, as they constitute violations of most military codes of conduct, ethics policies, and anti-corruption frameworks.

32 Joanne B. Ciulla, 'Review: In Praise of Nepotism?', Reviewed work: In Praise of Nepotism: A Natural History by Adam Bellow. *Business Ethics Quarterly*, Vol. 15: No. 1 (January 2005), pp. 153-60.

Table 2. The differences between nepotism, favouritism, and cronyism

Difference	Nepotism	Favouritism	Cronyism
Primary basis	Family relationship	Personal preference or bias	Loyalty and friendship
Scope	Limited to relatives	Broad – any individual	Typically friends/close allies
Typical impact	Promotion of unqualified relative	Skewed distribution of opportunities	Entrenchment of unaccountable networks
Legal status	Often explicitly prohibited	May be harder to prove	Often implied, hard to regulate

Detecting and evaluating cases of nepotism is often challenging. In one instance, the appointment of a senior military figure to a high-level defence leadership position raised concerns due to the individual's close personal connections with a top political office holder. The two were linked through a familial-style relationship, prompting questions about whether the selection was based on merit or personal affinity. In smaller countries, where social networks and cultural norms naturally create overlapping personal and professional ties, such situations are not uncommon, and they can make it difficult to distinguish legitimate appointments from those influenced by favouritism.

Ethical implications of nepotism

In one notable case within a national armed force, a senior military leader was suspended after allegations of nepotism emerged. Investigations found that the officer had manipulated recruitment and professional development processes to advantage a close personal associate, including altering admission criteria for an advanced military education programme and creating a position tailored to that individual's qualifications. The officer was later convicted of abuse of office and received a custodial sentence.

The practice of nepotism appears to result in an arbitrary exercise of power by the official granting the favours. It undermines faith, trust, and overall morale among the other members of the organization who witness it, as well as eroding public confidence in the organization that tolerates the practice. The practice of nepotism often results in unqualified beneficiaries being placed in positions beyond their competence. For this reason, nepotism has been condemned since ancient times as a serious form of political corruption that is invariably damaging to society.

> Military joke: Why does a good colonel's son have no chance of becoming a general? Because every general already has sons of their own.

Is nepotism illegal?

Nepotism poses the greatest risk when it involves the appointment of defence sector officials, as it significantly increases the potential for corruption and abuse of power. Therefore, primary accountability for nepotistic practices should lie with the officials responsible for such appointments. This perspective is supported by D.M. Safina, who argues that nepotism frequently results in the artificial creation of managerial roles or even entire departments to accommodate relatives.[33] Because of its general characterization as a serious form of

33 D.M. Safina, 'Corruption and Nepotism: The Inevitable Consequence of Social and Economic Changes', *Middle-East Journal of Scientific Research*, Vol. 13 (Special Issue of Socio-Economic Sciences and Humanities) (2013), pp.123–9.

political corruption and abuse of power, and because of its manifold harmful consequences on competence, morale, and public trust, most domestic legal jurisdictions will have laws preventing (or at least limiting) the practice, and most professional organizations (medical, military, law, the clergy, etc.) enforce codes of conduct that explicitly prohibit nepotism. The variations will come in the extent to which such laws and regulations are recognized and enforced in a given country or military service. The international anti-corruption organization Transparency International uses the degree of toleration and official lenience towards the practice of nepotism as one of its key measures of government and organizational corruption.

Is nepotism inherently unethical, or does the context matter?

You should abstain from the practice and delegate any such powers of selection or decision-making to another member of government or the organization when family and friends are involved, to avoid constituting a 'conflict of interest'. Inasmuch as laws and regulations, as discussed earlier, establish the most rudimentary baseline for permissible conduct, it seems that the general prohibition of nepotism usually, if not always, renders it wrong in practice.

Nepotism is not a sustainable model for defence sector governance, but in high-risk or post-crisis contexts, it appears more visible. One can claim that personnel recruited through family ties may feel increased pressure to follow the rules and perform their duties properly, knowing they are under greater scrutiny from their colleagues. Appointing close, trusted individuals (including family members) to sensitive roles one can ensure loyalty and a reduced risk of betrayal. However this approach typically results in unqualified promotions, lowered morale and public trust, and even the creation of unnecessary positions for relatives. Such practices undermine operational effectiveness, breach ethical standards, and lead to a misuse of resources.

> In some countries, children follow their parents into military service not because of corruption or favouritism, but because of shared identity, tradition, and deeply held values passed from one generation to the next. This should not be confused with nepotism.

Good practice or solution?

It is remarkable from a psychological standpoint how easily any one of us can ingeniously persuade ourselves that 'our situation' constitutes a special case, an exception to the norms and rules that apply to everyone else. We face a severe 'test of integrity' if we are tempted to engage in this practice by regarding our own situation as an exception to the legal and moral principles that prohibit nepotism.

A real story: Nepotism shaped by cultural tradition

Historically, in many societies, family or tribal loyalty ensured survival. This often resulted in nepotism being socially accepted and rarely perceived as negative. Such forms of nepotism have survived until modern times.

A senior officer once requested from his superior that a recruit from his village be promoted, citing social expectations rather than merit. Though well-intentioned, this request represented nepotism and revealed gaps in ethical education. The request, if materialized, would have presented a legal violation. Additionally, the incident underscores the need to address culturally rooted practices through improved education, training and awareness.

A test of integrity differs from a 'moral dilemma' in important ways. With a moral dilemma, people of good character are genuinely perplexed about what is the right thing to do. Here, by contrast, the right course of action is quite clear: *you should not engage in nepotism by using your privileged or powerful position to do arbitrary favours for family and friends.*

It is natural to be concerned that family members or friends who feel disadvantaged by an impartial decision may be disappointed or upset. They may even claim that you are neglecting your obligations to them and suggest that your position of authority should be used to grant them special favours, but such expectations are misguided. Any individual who puts pressure on you to engage in preferential treatment is placing an unfair and inappropriate burden on you. This is not a moral dilemma; it is a failure on their part to uphold basic standards of integrity. Your duty is not to advance the private interests of acquaintances or relatives, but to serve the public faithfully, adhere to the law, and maintain the highest standards of professional conduct. Nepotism is incompatible with these obligations. It is never a marker of integrity and, almost without exception, constitutes a clear violation of both personal and professional ethical norms.

Remember that

- Nepotism = favouring family or associates over merit.
- It remains common, even in modern democracies.
- In defence institutions, it harms competence, morale, trust, and efficiency.
- It is widely treated as corruption, though enforcement varies.
- Rejecting nepotism is an integrity test — leaders must prioritise ethics over personal loyalty.

Check-your-skills exercises

Task 1. 'One word, many faces of nepotism'

Objectives:

- To explore how participants understand and interpret nepotism in diverse contexts.
- To identify common themes, misconceptions, and emotional reactions to nepotism.
- To open up dialogue about personal experiences, moral conflict, and institutional impacts.
- To encourage critical reflection on why nepotism persists and how to resist it.

Duration: 45–60 minutes

Group size: 10–25 participants

Materials needed:

- A4 paper sheets or sticky notes (one per participant)
- Markers or pens
- Wall or board space to display the sheets
- Tape or magnets (if not using sticky notes)
- Flipchart or whiteboard for grouping themes

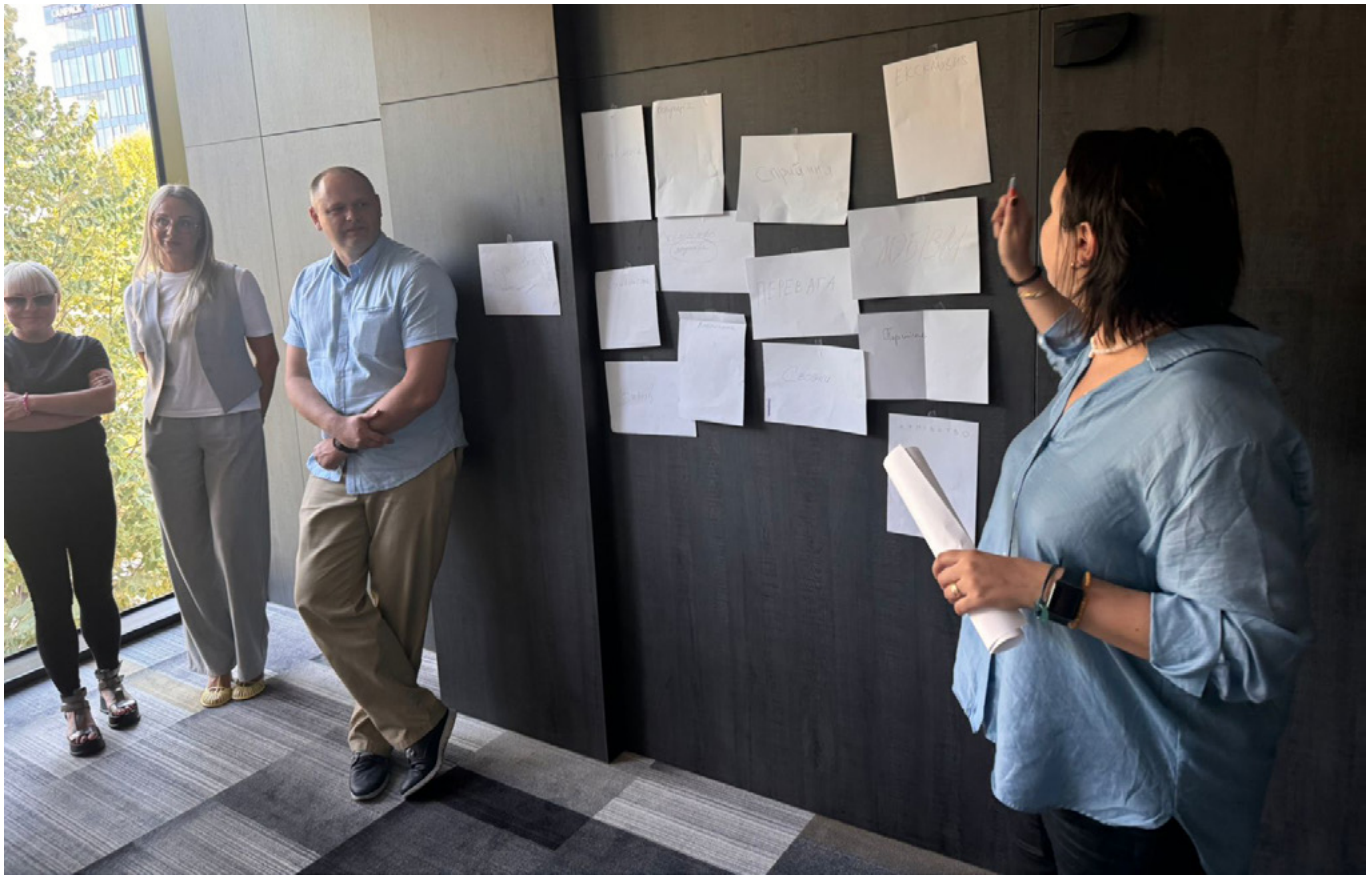

Figure 5. 'One word, many faces of nepotism' exercise in practice

© Photo: Grazvydas Jasutis

Instructions:

1. Introduction (5 minutes):

- The instructor briefly introduces the activity: *'Nepotism can appear in many forms and contexts. Before we dive into its formal definitions and legal frameworks, I want to explore how each of us personally perceives this issue.'*

2. The one-word task (5–7 minutes):

- Ask each participant to: *'Think about nepotism and write down one word that comes to mind. It could be a feeling, a consequence, a value, or a keyword – anything you associate with the concept.'*
- Remind the participants: *'There are no wrong answers – this is about your personal reaction.'*

3. Wall display (5 minutes):

- One by one, participants come up to the wall and place their paper so that everyone can see it.
- Encourage them to read each other's words as they are posted.

4. Observation and grouping (10–15 minutes):

- The instructor reviews the wall and begins grouping similar words (e.g. 'corruption', 'injustice', 'unfairness' may be grouped as ethical concerns).
- Ask: *'What do you notice about these words? Are there clusters? Peculiarities?'*
- Use a flipchart or whiteboard to sketch out thematic categories (e.g. emotions, consequences, systems, resistance).

5. Facilitated discussion (15 minutes):

- Lead a group discussion using guiding questions:
  - Why do you think these themes came up?
  - Do you see more emotional or structural interpretations?
  - Did any of the words surprise you?
  - What does the variety of words tell us about how we experience or witness nepotism?

6. Personal reflections and sharing (optional but powerful – 10–15 minutes):

- Invite volunteers to share personal or professional anecdotes: *'Have you ever witnessed or been affected by nepotism? How did it have an impact on you or the organization?'*
- Remind participants of the ground rules for confidentiality and respect.

Expected outcomes:

- Visual mapping of how participants collectively perceive nepotism.
- Identification of common emotional responses (anger, frustration, betrayal, resignation).
- Emergence of systemic insights (e.g. how nepotism links to corruption, inequality, favouritism).
- Realization of moral conflict (e.g. balancing loyalty to family vs fairness).
- Increased empathy and peer learning through personal stories.
- Foundation for further modules on COI, integrity, and anti-corruption strategies.

3.3. Misuse of command authority and unprofessional behaviour

Module objectives

To equip defence sector personnel with the knowledge, analytical skills, and ethical awareness necessary to identify, prevent, and respond to abuse of authority and unprofessional conduct in military contexts, thereby fostering integrity, discipline, and respect for human dignity in all aspects of service.

Key information

a. Abuse of authority occurs when individuals in positions of command or influence misuse their power in ways that harm subordinates, peers, or the institution itself. This can take many forms, from overt acts of verbal harassment or physical intimidation to more subtle behaviour such as unfair tasking, denial of opportunities, or the manipulation of rules for personal gain.

b. Professionalism is the cornerstone of effective military service, requiring conduct that upholds dignity, discipline, and mutual respect at all times, both on and off duty. In contrast, unprofessional behaviour – whether it is fraternization, public intoxication, abuse of rank, or showing blatant favouritism – weakens the moral authority of leaders and damages the trust essential for operational effectiveness.

c. Legal and ethical boundaries are central to understanding these issues. Some forms of abuse, such as sexual assault, hazing, or cruelty, are clear criminal offences under both military and civilian law. Others, while not explicitly illegal, still breach codes of ethics and professional standards, and can undermine institutional values and require decisive leadership intervention.

d. The impact of abuse of authority on unit cohesion and mission success is profound. Trust, morale, and discipline are paramount to an effective fighting force, and once compromised, they are difficult to restore. Abuse not only weakens readiness and operational performance but can also inflict lasting reputational damage on the armed forces, reducing public confidence in the institution.

e. Command positions bring recurring ethical temptations. Leaders may be tempted to misuse funds, grant favours in exchange for loyalty, enter into inappropriate relationships, or ignore misconduct to avoid conflict.

f. Finally, all military personnel have both a moral and legal duty to report abuse of authority and to resist unlawful orders. Failure to report in the face of misconduct allows the problem to persist and signals a tolerance for unacceptable behaviour.

Module content

Abuse of power and unprofessional behaviour

Military rank brings both authority and ethical risk. A familiar old proverb warns that power tends to corrupt, and absolute power corrupts absolutely.

Misuse of command authority can take many forms. Many countries have explicit statutes within military law which prohibit any use of power that injures a subordinate, is manifestly unfair, or undermines good order and discipline.

'Cruelty and Maltreatment' Article 93 of the U.S. military code forbids 30 acts of forms of misuse of authority[34], which can be grouped into 8 categories:

- Violence and physical abuse
- Sexual misconduct
- Psychological and emotional abuse
- Coercive hazing and forced acts
- Authority abuse and procedural violations
- Neglect and denial of basic needs
- Discrimination and unfair treatment
- Endangerment and operational misconduct

Categorizing misuse of authority in this way highlights patterns of misconduct and discriminatory practices, rather than viewing each act in isolation, and makes it easier to identify systemic issues, as well as develop targeted training and oversight mechanisms.

'Professionalism' incorporates a wide variety of behaviours, whether precisely specified or more intuitively defined, of uniformed personnel who engage in the service of their country. Hence, we could simply denounce all forms of misconduct, from nepotism and bribery to discrimination and abuse of power, as 'unprofessional'. Some experts claim that unprofessionalism refers to conduct that fails to meet expected norms or standards but does *not necessarily involve power misuse.* For instance, unprofessional behaviour in the military includes verbal abuse, intimidating body language, and bullying – all actions that demean, frighten, or single out subordinates without involving formal misuse of command authority. These behaviours undermine morale, create fear, and can lead to serious psychological harm when left unaddressed. Abuse of authority, however, includes unfair denial of leave, improper punishment, assigning personal errands to subordinates, creating a hostile work environment, bypassing the rules, unauthorized disclosure of sensitive information, and making unreasonable demands. For instance, during a military deployment, a service member was denied emergency leave by the chain of command despite multiple appeals and official verification that an immediate family member required critical medical treatment (*arbitrary refusal of a right controlled only by command authority*). This denial of emergency leave was allegedly motivated by retaliation or bias. This incident, along with similar cases, has raised broader concerns about inconsistent application of emergency leave policies and delays in processing requests, contributing to demoralization among personnel. This goes beyond unprofessionalism by involving the deliberate misuse of command power and official responsibilities.

34 10 U.S. Code § 893 – Art. 93. *Cruelty and maltreatment*. Available at: https://www.law.cornell.edu/uscode/text/10/893

The military hierarchy relies on authority that goes with rank and position, and the obedience of those within the chain of command. Without command authority and unhesitating obedience to it, the military could not function efficiently in wartime. However, command authority is limited. If the exercise of authority is self-serving, arbitrary, or inconsistent, it is incompatible with the mission of the military. Abuse of authority and position is also *unethical*. As already discussed, ethics requires that human dignity be respected; cruelty, bullying, or other degrading treatment violate this principle. Historically, new members of military organizations were routinely subjected to harassment, hazing, and demeaning assignments for the purpose of weeding out the 'weak' or the 'cowardly'. According to sociologists, hazing also serves to break down new members psychologically, dismantling their old identity and instilling in them the group's norms. Most military organizations nowadays do not tolerate humiliation or abuse, and consider any form of it, including initiation rites, to involve misuse of command authority. Whatever the cause, cases of abuse of power constitute yet another pitfall in the path to discipline, good order, and the proper functioning of military organizations.

Temptations of military leadership

Research has been carried out by scholars to examine ethical challenges faced by mid-level military leaders. Drawing on field interviews, leadership assessments, and real-world case studies, the scholars analysed how individuals in command roles experience and respond to ethical pressures. Their work highlights recurring patterns of misconduct, the organizational factors that enable them, and practical strategies leaders can use to recognize and resist ethical temptation. The findings were publsished in *Joint Force Quarterly*, providing evidence-based insights aimed at strengthening integrity within the profession of arms.

Some information from this research is included in Annex I.

Longenecker, C. and Shufelt, J.W., 'Conquering the Ethical Temptations of Command: Lessons from the Field Grades', *Joint Force Quarterly*, Vol. 101 (31 March 2021). Available at: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2553439/conquering-the-ethical-temptations-of-command-lessons-from-the-field-gradess

Bullying and humiliating junior officers or forcing them to perform servile tasks that are not part of their official military duties is a common form of abuse of power in certain countries (e.g. ordering subordinates to pick up the CO's uniforms from the laundry, or to chauffeur the CO's spouse on a shopping trip). Exercising one's military rank to force a subordinate (military or civilian) into engaging in a sexual relationship is another, regrettably familiar, form of this abuse. This leads to a breakdown in command climate, undermining trust, morale, and the legitimacy of leadership. Leadership requires both authority and restraint, and that misuse of rank – whether through coercion, fraternization, or hazing – erodes the ethical foundations essential for military cohesion and effectiveness.

Is abuse of power illegal?

The non-criminal but unethical misuse of authority is usually covered in military standards and regulations and falls under the category of professionalism and unprofessional behaviour. Specific and particularly horrific forms of abuse, such as rape and sexual assault, however, are outlined and expressly prohibited in domestic and military criminal law. Harassment (such as stalking or pressurizing subordinates into unwanted personal relationships) may not be crimes, but they are prohibited, and the victims protected, under codes governing appropriate behaviour in the workplace. Quid pro quo proposals ('I'll see you are promoted or receive a pay increase if you go on a date with me') are specifically pinpointed and prohibited in most jurisdictions.

A former senior government official was convicted of embezzlement and fraud after an investigation revealed that public funds had been used to cover a variety of personal expenses unrelated to official duties. These included costs associated with childcare, private transportation, and the purchase and delivery of personal goods. The official was aware that these activities did not fall within the remit of government staff.

According to the findings, the individual had also used an official fuel card for private purposes and authorized the payment of catering and other services for a personal birthday celebration using public money. Additional costs – such as travel expenses for a family member, the purchase of household equipment, and expenses linked to attending recreational events – were likewise charged to the public budget.

The court determined that most of the allegations were substantiated. The expenditure related to childcare was especially contentious, though, and the court noted that personal family-related costs could not be lawfully covered by public funds. Attempts during the trial to frame the official's family travel as work-related were deemed to be efforts to exploit the goodwill of government staff, and the court held that the official had used employees' working hours and personal time, as well as public resources, to resolve private family matters.

The defence argued that the duties of drivers and advisers included supporting the official's family and therefore the assignments were lawful. The court rejected this interpretation as artificial and unfounded, emphasizing that although the workday of a senior official may be long and demanding, this does not entitle them to benefit from publicly funded personal or family support, nor to impose such obligations on staff.

The court terminated proceedings on one charge – misuse of a fuel card – classifying it instead as a minor offence. Costs related to the use of an official vehicle could not be addressed because they were not included in the indictment.

Similar misuse of authority in defence institutions – such as assigning personal tasks to subordinates or misusing operational resources – is likewise subject to disciplinary or legal action.

Abuse of power as a test of integrity

The authority given to an officer as part of their duties may enable them to coerce a subordinate to act against their will. Free will, however, is part of the very essence of being human – it is sacrosanct and must be respected. Accordingly, the orders of a military commander may not transgress the values a soldier has voluntarily espoused in their oath. That is, if a commanding officer asks a subordinate to act in a way that does not serve national security, or that does not serve the people of their country, that commander is abusing their authority. The nature of the superior's official position places them in a unique situation of dominance and control, so they have a moral obligation to refrain from manipulating those under their command.

Ethical decision-making under pressure is important in defence structures. Ethical lapses at senior levels often reflect failures in both individual character and institutional accountability. If we agree with Lord Acton that opportunity and temptation to engage in such behaviour invariably accompany the loosening of accountability that comes with high rank, we likewise demand as a matter of professional comportment that those in power can and must refrain from such behaviour. To do otherwise is, once again, to fail a profound test of integrity. The ability to resist abusing power is a core requirement of professional military leadership and a direct indicator of integrity.

Remember that

- Abuse of authority is misuse of power that harms people or the institution.
- Professionalism demands dignity, discipline, and respect – unprofessional conduct erodes trust.
- Some abuses are criminal; others breach ethics and require leadership action.
- Abuse damages morale, cohesion, readiness, and institutional reputation.
- Leadership roles carry ongoing ethical temptations – integrity must prevail.
- All personnel have a duty to report abuse and refuse unlawful orders.

Check-your-skills exercises

Task 1. Filming exercise: Abuse of authority and unprofessionalism

Objective:

To help participants apply concepts from the lesson by role-playing realistic military scenarios involving abuse of authority or unprofessional conduct. Each group will be allocated a unique scenario, must prepare a response, and act it out while the facilitator films their performance. The recordings will be reviewed together, allowing for discussion, feedback, and reinforcement of key learning points.

Instructions:

1. Divide participants into three groups.
2. Provide each group with their assigned scenario.
3. Allow 15 minutes for group discussion and preparation of their role-play response.
4. Film each group's performance (3–5 minutes each).
5. Replay the recordings to the entire class and guide a discussion using the lesson's ethical framework.

Scenario 1: Coercive tasking and public humiliation

A company commander, frustrated with a soldier's repeated mistakes, orders them to perform an exhausting and unrelated physical task as punishment during the rehearsal for an official parade. The commander shouts insults in front of peers and junior soldiers, making jokes about the soldier's lack of ability.

Group task:

Role-play the scene, then demonstrate how a professional leader or bystander could intervene appropriately to address the situation without undermining discipline.

Key discussion points after viewing:

- Did the commander's conduct fall within professional and legal boundaries?
- How could corrective measures have been implemented respectfully?
- What are the consequences of public humiliation for morale and cohesion?

Scenario 2: Misuse of resources for personal gain

A logistics officer orders subordinates to use military vehicles and fuel to transport furniture to their private residence. When questioned by the subordinates about this, the officer implies that refusal will lead to poor performance evaluations and denial of leave.

Group task:

Act out the conversation between the officer and subordinates, and then provide a constructive, integrity-based response from the perspective of a subordinate who recognizes the misuse of authority.

Key discussion points after viewing:

- What risks do subordinates face in refusing such orders?
- What reporting mechanisms should be used?
- How does misuse of resources undermine trust in leadership?

Scenario 3: Lack of responsiveness from senior leadership

You are a senior officer working on an urgent procurement project that requires approval from the Deputy Minister of Defence. Despite multiple follow-ups over several weeks, the Deputy Minister has not responded to your emails or official memos. The delay is beginning to have an impact on contract deadlines, troop readiness, and budget allocation. Your team is growing frustrated, and partner organizations are pressing for answers.

Group task:

Role-play the situation in two parts:

1. An internal team meeting where frustration is voiced and possible approaches are discussed.
2. An escalation scenario where the issue is formally raised through alternative channels while maintaining professionalism and respect for the chain of command.

Key discussion points after viewing:

- What are appropriate ways to escalate an issue when senior leadership is unresponsive?
- How do you balance urgency with respect for hierarchical authority?
- What communication strategies can improve the chances of receiving a timely response without creating conflict?

3.4. Gifts and bribes

Module objectives

Participants will understand the ethical distinction between acceptable gift-giving, inappropriate transactional gifts, and outright bribery in military and professional contexts. They will learn to recognize the impact of corruption on organizational integrity, morale, and public trust, and practise applying professional judgement when confronted with such dilemmas.

Key information

a. Gifts as part of social and professional life. Gift-giving is common across cultures for occasions such as birthdays, weddings, and other occasions. In many cases, it is an expression of goodwill and relationship-building. Recognizing the difference between culturally appropriate gestures and ethically questionable actions is the first step towards sound professional conduct.

b. When gifts cross the ethical line. A gift becomes problematic if it creates a sense of obligation or is given with the intent of influencing official decisions. Even if no explicit request is made, the perception of favouritism or bias can undermine fairness and institutional credibility.

c. Transactional arrangements and favouritism. When a gift is tied to an expected outcome – such as a promotion, favourable assignment, or leniency – it is no longer a gesture of kindness but an unethical transactional exchange. Such arrangements foster favouritism, damage trust among peers, and weaken merit-based systems.

d. Bribes as corruption in action. Unlike questionable gifts, bribes are deliberate attempts to distort official duties. Bribes can involve money, favours, or material benefits offered to secure an advantage or avoid a penalty. In military contexts, this may involve recruitment, procurement, or interpretation of code of conduct – all of which directly impact fairness, security, and discipline.

e. Impact of corruption on institutions. Bribery and disguised gift-giving erode organizational integrity. They discourage merit, foster mediocrity, and fuel public distrust. In militaries, corruption damages morale, undermines command authority, and can compromise mission effectiveness.

f. Cultural relativism vs universal professional standards. Bribery is sometimes defended as a cultural norm or ‘the way business is done’. However, previous cases (e.g. politicians ousted for taking bribes despite cultural tolerance) show that citizens often reject corruption when provided with transparency and accountability. Professional standards must transcend cultural excuses.

g. Professional responsibility and moral courage. Ethical military and professional conduct means refusing to give or accept bribes, reporting corruption where possible, and fostering a culture of integrity. This often requires moral courage – the willingness to act ethically despite risks of retaliation or isolation. Whistle-blowing, though difficult, strengthens professionalism and accountability.

Module content

Ordinary people, including military personnel, give and receive gifts all the time; birthdays, weddings, promotions, special holidays – all these events are frequently accompanied by the giving and receiving of presents between family, friends, and co-workers.

Unless there is some reciprocal expectation on the part of the donor (gift-giver): praise, currying favour, or exerting some type of inappropriate influence on decision-making by the recipient, then giving or receiving a gift is not wrong. Sometimes, though, the line between appropriate and inappropriate gift-giving can be difficult to discern, in part because this may depend upon the intentions behind the giving, and that intention can be hard to pin down.

Dilemma: Balancing integrity and diplomacy

A high-ranking delegation from the Ministry of Defence go on an official visit to the Middle East with the purpose of establishing cooperation. The visit is straightforward, without hidden agendas or negotiations. During the visit, the hosts present each delegation member with a MacBook as a gift. This gesture, while generous, creates a dilemma. On the one hand, refusing the gift would be perceived as a cultural offence. In the country which the delegation is visiting, gift-giving is an important tradition, and declining such a gesture could be taken as an insult, undermining goodwill and trust between the partners. On the other hand, accepting the MacBooks is problematic from the perspective of integrity and professional standards. Many ministries of defence, particularly in NATO and EU countries, operate under strict codes of conduct which prohibit officials from accepting gifts of significant value. A MacBook clearly goes beyond the category of symbolic or token gifts and could be seen as an attempt to exert influence, raising concerns about COI, corruption, or breach of rules. Thus, the delegation faces a dilemma: to accept the gift and risk violating their own integrity standards, or to refuse it and risk damaging the bilateral relationship.

The dilemma can be resolved by finding a balance between respecting cultural traditions and upholding rules of integrity. The delegation can graciously accept the MacBooks in the moment, acknowledging the gift as a symbol of friendship and cooperation, so as not to offend the hosts. However, rather than keeping them for personal use, the delegation should formally register the items as state property upon return. Many ministries have procedures for handling such situations: gifts of significant value are logged, declared, and either stored, displayed, or allocated for official institutional use rather than being treated as personal possessions.

Gifts as transactional arrangements

The threshold of wrongful intent is crossed when a gift is provided with the expectation of receiving something in return, creating what may be described as a *transactional* arrangement. For example, offering a commanding officer an expensive bottle of preferred brandy shortly before that officer is due to consider the giver for promotion is inappropriate. In such circumstances, the gift should not be offered, nor should it be accepted. This act would be seen as an inappropriate transactional arrangement.

Accordingly, the giving of gifts to one's supervisors, and to other high-ranking officials, while not necessarily illegal, is often prohibited in military regulations because of the likelihood of corruption and the COI such gifts might lead to. Not so the other way round: a commanding officer is usually allowed to confer gifts on subordinates as part of a celebration, an act of kindness, or a reward for outstanding performance. But if such gift-giving occurs too frequently or lavishly, or without apparent reason, it may be that the commander is trying to 'buy popularity' or curry favour with the rank and file members of their command.

Notice how difficult it can be to assess intentions from actions, and how hard it would be to anticipate every possible form of corruption and legislate against it. As we observed in our treatment of law and morality earlier, it is best to foster a sense of mature and responsible judgement on the part of a military organization's members, so that we do not have to legislate every aspect of their lives and personal relationships (attempts to regulate do not necessarily lead to positive outcomes). When our personnel cannot determine right from wrong, or cannot be relied upon, we are then (as in many governments and militaries around the world) obliged to strengthen, clarify, and multiply our regulatory regime until it becomes cumbersome and suffocating. The saying in some military and government organizations is: 'If we simply do nothing at all, we will not do anything wrong.'

Bribes

These differ significantly from gifts, although it is important to recognize when gift-giving turns into bribery. A bribe is some special consideration of material value, most often money, either offered to or demanded from an official to perform that official's normal assigned responsibilities. Border guards and sentries posted between countries may demand some sort of gratuity in order to grant permission to legitimate travellers to cross. A citizen may offer a bribe to the tax collector in order for the latter to ignore an incorrectly filled-out tax return. A military recruiter, especially in a poor country where enlistment is a ticket to a lucrative job, may demand (or be offered) a bribe to grant the coveted position to the petitioner or applicant. Another widespread example is a conscription commission asking for a bribe to write a note of disability for a potential conscript.

Although definitions of bribery vary across institutions and jurisdictions, they all share a common thread: an official willingly breaching trust in exchange for some form of benefit. Transparency International defines bribery as the offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. Such inducements can take the form of money, gifts, loans, fees, rewards or other advantages, such as tax breaks, services, donations, or personal favours.[35] Similarly, Article 15 of the UN Convention against Corruption (UNCAC) defines bribery of public officials as 'the promise, offering or giving, to a public official, directly or indirectly, of an undue advantage, for the official himself or herself or another person or entity, in order that the official act or refrain from acting in the exercise of his or her official duties'.[36]

National legal systems adopt their own definitions of bribery. For example, the German Criminal Code broadly defines bribery as demanding, allowing oneself to be promised, or accepting an undue advantage for oneself or a third party in return for performing or refraining from performing an act, upon request or instruction, in the exercise of their mandate.[37] The Canadian Criminal Code takes a similarly broad view, providing that a person engages in bribery if they 'directly or indirectly, corruptly accept, obtain, agree to accept or attempt to obtain, for themselves or another person, [or give or offer] any money, valuable consideration, office, place or employment in respect of anything done or omitted or to be done or omitted by them in their official capacity'.[38] In Ukraine, the term 'bribe' has been removed from the legislation and replaced with the broader concept of an 'unlawful benefit'. As clarified in Articles 368–370 of the Criminal Code of Ukraine, such unlawful benefit may include monetary assets (cash or non-cash transfers), service provision, valuables (e.g. jewellery, works of art), or other tangible assets.[39]

35 Transparency International UK, '5. What Is Bribery?' (2024), https://www.antibriberyguidance.org/guidance/5-what-bribery/guidance

36 UN General Assembly, United Nations Convention Against Corruption, A/58/422 (31 October 2003), https://www.refworld.org/legal/agreements/unga/2003/en/21418

37 German Criminal Code, 108e (1) §, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p3276

38 Criminal Code (R.S.C., 1985, c. C-46), s.119 (2007), https://laws-lois.justice.gc.ca/eng/acts/C-46/page-22.html#h-117813

39 Олексій Панасенко, "Затримали за хабар? Що робити?," Prikhodko&Partners, January 12, 2023, https://prikhodko.com.ua/my-i-zmi/my-i-zmi/stattya/zatrymaly-za-habar-shho-robyty/

It is worth touching on culture and its impact on bribery. Several decades ago, the CEO of a major aerospace company was found to have transported large sums of cash, concealed in paper bags, as 'gifts' intended for the head of government of another state, with the objective of securing favourable treatment. At the time, some observers dismissed the incident as an example of moral or cultural relativism, suggesting such practices were simply part of local business customs. This argument is often given in defence of turning a blind eye towards the practice of bribery. Interestingly, however, when the citizens of the country in our example discovered what their prime minister had been involved in, they voted him out of office and sent him to jail – so much for the claim that bribery was 'accepted routine practice' in that country. Meanwhile, the CEO was given a prison sentence in his home country, where bribery (including bribery of foreign governments) was illegal and defined as a shamefully corrupt practice. Those who defend this type of practice are usually those who profit from it, not those (ordinary citizens and taxpayers) who are collectively harmed by it.

Dilemma: Operational expediency or institutional credibility?

A similar dilemma arises in contexts where administrative systems are highly complex and slow, making it difficult for officials to move equipment, secure permits, or gain access to facilities in a timely manner. An official working on a defence-related project is under pressure to deliver results quickly, whether it be moving equipment across provinces, securing construction permits, or arranging access to a government facility. The bureaucratic rules in place are meant to ensure transparency and accountability, but in practice they are slow, fragmented, and frustrating. At the same time, an opportunity presents itself: by paying a bribe to an intermediary or local authority, the official could bypass the obstacles, obtain the necessary clearances, and move the project forward without delay. The temptation is strong, because doing so would allow the mission to succeed on schedule, demonstrate efficiency to superiors, and show tangible progress on the ground. Yet, engaging in bribery carries serious risks. It undermines personal and institutional integrity, violates both national and international anti-corruption laws, and contributes to the very cycle of corruption that weakens governance and security in the country. It also exposes the official and the organization to reputational damage, possible sanctions, or criminal liability. The official is therefore caught in a dilemma: whether to take the seemingly expedient path that secures short-term organizational success, or to uphold ethical and legal standards, accepting delays and complications but protecting long-term credibility and the principle of accountability.

Corruption in peacekeeping

Instances of corruption have also been documented in the selection processes for international peacekeeping missions, where deployment opportunities are often considered financially desirable. In several cases, military recruiters have been detained for accepting or demanding payments in exchange for adding individuals to peacekeeping contingents. These incidents involved service members who were seeking assignment to UN missions abroad and who offered sums ranging from modest amounts to several thousand dollars. Such cases illustrate how the prospect of lucrative deployment can create incentives for bribery within selection systems that lack adequate oversight.

The best professional practice, when confronted by demands to pay a bribe or turn a blind eye to the 'custom' of bribery in one's own country or organization, is therefore to refuse. Don't request a bribe, don't pay or offer to pay a bribe, and do your utmost to combat this corrupt practice. That said, it is possible to imagine a moral dilemma arising from circumstances in which one is personally powerless or helpless either to refuse to cooperate, or to put a stop to the practice. The dilemma itself then becomes whether or not to bring official charges against the perpetrator, or report the corruption itself to appropriate authorities, especially if there may be a serious risk of retaliation against the 'whistle-blower' – that is, the alleged victim of the bribery scheme who sounds the alarm and reports the incident to proper authorities and the public. To do so constitutes an act of moral courage and professionalism, which leads us to the activities for this module.

Remember that

- ✓ Gift-giving can be culturally normal – ethics require knowing when it crosses the line.
- ✓ A gift becomes unethical when it creates obligation or influences decisions.
- ✓ Gifts tied to outcomes are transactional and undermine fairness and merit.
- ✓ Bribes intentionally distort duty – they threaten discipline, security, and justice.
- ✓ Professional standards outweigh cultural excuses for bribery.
- ✓ Ethical conduct requires refusing, reporting, and showing moral courage.

Check-your-skills exercises

Task 1. Simulation exercise: 'Gift or bribe?'

Structure:

Divide participants into small groups. Provide each with realistic case scenarios. Examples:

- A soldier gives a commanding officer a bottle of expensive alcohol before a promotion review.
- A border guard demands 'extra money' from civilians to cross a checkpoint.
- A commander regularly distributes lavish gifts to subordinates.
- A procurement officer is offered tickets to a sports event by a supplier.
- A captain offers a concert ticket to a battalion commander.

Activity:

Groups classify the situation as: legitimate gift, transactional gift, or bribe. They must justify their reasoning and propose a professional response.

Outcome:

Participants gain practice in spotting the difference between harmless customs and corruption, while also exploring 'grey areas'.

Task 2. Group task: The peacekeeping dilemma

Instructions for facilitator:

1. Divide participants into small groups (3–5 people).
2. Present the following scenario:
   - Imagine you are a young and ambitious officer eager to partake in a UN peacekeeping mission. You receive information that your chances of being selected will significantly improve if you make a payment to the official in charge of assignments. Do you choose to report the bribery, knowing this could potentially jeopardize your career prospects and cost you the opportunity to serve abroad? Do you pay, justifying your decision by the fact that 'everyone does it' and that the benefits of deployment outweigh the risks? What ethical principles and legal considerations should guide your choice?
3. Ask groups to discuss and answer the following questions (write them on a flipchart/slide):
   - What are the short – and long-term consequences of each choice (reporting vs paying vs ignoring)?
   - What ethical principles are at stake (integrity, fairness, professional duty, loyalty, etc.)?
   - What legal obligations exist in such situations under national and international law?
   - How might corruption in peacekeeping assignments affect the credibility of national armed forces working abroad?
   - If you were talking to a friend facing this dilemma, what would you advise them to do?
4. Debrief in plenary:
   - Invite each group to briefly present their reasoning.
   - Summarize the key ethical and legal principles discussed (e.g. rule of law, anti-corruption standards, professional integrity, responsibility to the institution and the state).
   - Highlight that systemic issues (e.g. corruption in peacekeeping selection) harm not only individuals but also institutional trust and international reputation.

Duration: 30–40 minutes (20 minutes for group work, 15 minutes for plenary debrief, and 5 minutes for wrap-up).

Expected outcomes:

Participants recognize the complexity of such dilemmas, weigh ethical vs pragmatic choices, and deepen their understanding of the personal and institutional impact of corruption in peacekeeping missions.

3.5. Conflict of interest in the defence sector

Obliti privatorum publica curate (Forget private affairs; take care of public ones).

– From a 17th century inscription above the Rector's Palace in Dubrovnik

Module objectives

To enhance participants' understanding of conflict of interest (COI) in the defence sector; the implications for integrity and public trust; and practical measures to prevent, identify, and manage such situations in both military and civilian contexts.

Key information

a. A COI arises when an individual's private interests, financial, familial, political, or otherwise, could improperly influence, or appear to influence, the impartial execution of their official duties. The concept includes:

- Actual COI: A direct conflict between official duties and personal interest
- Perceived COI: A situation that may not involve misconduct but could reasonably be seen as compromising integrity
- Potential COI: Circumstances where a future conflict could arise. In the defence sector, these situations can damage institutional credibility even when no wrongdoing has occurred.

b. Defence institutions are particularly vulnerable because of their authority, large budgets, and operational secrecy. COIs can emerge in awarding contracts to companies where an official has financial stakes; in advancing relatives, friends, or personal allies without merit-based justification; or in allowing personal or corporate ties to shape strategic or tactical decisions. The security environment often magnifies the impact, as biased decisions can endanger missions and lives.

c. COIs are often not outright illegal but they still pose ethical hazards. Even in the absence of unlawful acts, the appearance of compromised judgement can reduce trust in leadership, erode morale within the armed forces, and harm the institution's standing with the public and international partners. Ethical leadership requires proactive avoidance of situations that could give rise to such perceptions.

d. Some COIs are built into the structure of governance and require systemic solutions.

- Revolving-door phenomenon: movement of personnel between government positions and private industry
- Post-service lobbying: retired senior officials using insider knowledge and networks for corporate advantage.

Without safeguards, these patterns can undermine public confidence and create institutional dependencies on private-sector interests.

e. Strong institutional safeguards help prevent COIs from undermining integrity, for example mandatory disclosure of all financial and personal interests relevant to official duties; recusal requirements for decision-makers facing potential conflict; independent review boards to assess COI situations and ensure compliance with policy; and regular training on recognizing and managing COIs for both civilian and military personnel.

f. Effective COI management requires overlapping systems of accountability, such as:

- Legislation setting out clear COI definitions, penalties, and disclosure rules
- Institutional codes of conduct to reinforce ethical norms
- Internal oversight bodies (e.g. inspector-general offices) empowered to investigate complaints
- External oversight from parliaments, audit bodies, and civil society to ensure transparency.

g. Building a culture of integrity is as crucial as the existence of formal rules, as ethical norms guide behaviour in situations where laws or policies may not provide explicit direction.

Module content

We might note that nepotism itself is a very obvious example of COI; however, there are many more instances of COI than choosing whether to grant preferential treatment to associates. They arise, for example, when otherwise routine organizational decisions or policy secretly affect your own personal welfare. This can make COIs quite complex, pervasive, and (unlike nepotism) difficult to avoid completely.

Definitions

- A conflict of interest involves a conflict between the public duty and the private interest of a public official, in which the public official's private-capacity interest could improperly influence the performance of his/her official duties and responsibilities.[40]
- A conflict of interest is any situation where interference between a public interest and public or private interests is likely to influence or to appear to influence the independent, impartial, and objective exercise of a function.[41]
- In its broadest sense, a conflict of interest can be understood as any situation where an official's personal interests run contrary to their public duties. These can be situations where personal or family ties affect an official's impartiality in performing their public work. Similarly, a conflict may emerge if an official has other professional or commercial interests related to their public position.[42]

40 OECD, 'Conflict of Interest Policies and Practices in Nine EU Member States', SIGMA (31 December 2004), https://www.oecd.org/content/dam/oecd/en/publications/reports/2005/01/conflict-of-interest-policies-and-practices-in-nine-eu-member-states_g17a1def/5kml60r7g5zq-en.pdf

41 Légifrance. 'Article 2 – LOI N° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique' (2025), https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000035588428

42 Transparency International, 'Codes of Conduct in Defence Ministries and Armed Forces' (May 2011), https://ti-defence.org/wp-content/uploads/2016/03/1106_CodesofConduct.pdf

Where might conflicts of interest arise in the military?

Usually when examining COIs that arise in government, military, or commercial business practices, the 'interests' involved are **financial**. For example, as a senior commanding officer, you may have a duty to recommend one of two different geographical locations in your country to build a new military complex (a seaport, airbase, or army training facility). Based on the needs of the service itself, as well as costs of acquisition and construction, and other logistical factors, the first of the two locations may well, in your expert opinion, be the superior location for this new facility. However, the second location is, from those perspectives, *almost* as good (perhaps it will cost a bit more or offer a few less strategic advantages than the first location).

Unbeknown to those who are depending upon your expert advice, however, your spouse has just inherited a large farm in their parents' will, adjacent to the second location. It is not titled in your name in public records, so no one else knows about this situation yet. While it is not worth a great deal of money now, if your government decided to build the new military facility in that second, slightly less ideal location, the farm would vastly increase in value by providing much-needed space to construct new housing and schools for military families, as well as real estate for new businesses that would want to locate in that area to serve the military complex itself.

This may well lead to a COI. The conflict involves your responsibility to make the best decision, impartially, in terms of military requirements and available public resources. But those considerations seem at odds, in this instance, with your own personal and financial welfare. You are not at fault for finding yourself in this situation, but if you do not act appropriately now that you have recognized the problem, you may be subject to ethical violations or disciplinary actions.

Notably, the conflict illustrated in the example above could persist even if that second location turned out to be the best choice, solely in light of the relevant military and public interests involved. Now you personally stand to benefit financially even while you seemingly discharge your primary duty to recommend the best choice for the military and the government. Nonetheless, when making your recommendation, there are still 'interests' (your own) that are different (even if not now in direct opposition) from those of the public and military you serve. Even if you claim to have ignored your own interests in making your recommendation, it will certainly at least *appear* to others that you may have engaged in misconduct.

Examples of conflict of interest

Concerns about COIs have arisen in several high-level defence procurement and diplomatic contexts. In one case, a senior leader of a federally funded research organization participated in a study evaluating whether a major aircraft programme met the criteria for a multi-year procurement strategy, despite simultaneously holding a board position at a company with financial interests in that programme. An inspector-general later determined that this dual role violated COI standards, and although no evidence indicated any influence on the study's findings, the individual subsequently resigned from both positions.

In another instance, a retired senior military officer was appointed as a special envoy on a security issue while also serving on the board of a major defence contractor and an industry advisory body. The overlap between these roles prompted criticism that such arrangements created structural COIs, particularly given ongoing and recently concluded arms sales involving the same defence company. Observers argued that this alignment of responsibilities risked blurring the boundary between official duties and private-sector interests.

The third example is linked to corruption in private military and security companies (PMSCs). PMSCs played a major role in supporting international operations during two decades of counterinsurgency and stabilization efforts. However, numerous oversight bodies and investigative authorities documented widespread corruption involving private contractors.

In one case, a major firm agreed to a financial settlement after allegations that its personnel had inflated costs and accepted kickbacks from subcontractors in connection with security-training support. In another instance, two locally based PMSCs with close links to political elites were contracted as convoy escorts but were later investigated for using international funds to pay armed groups for safe passage and for staging fabricated attacks to justify their continued employment. Despite evidence of collusion with insurgent elements and mistreatment of civilians, these companies were eventually permitted to resume operations after temporary suspension.

Such practices contributed to financial losses, operational shortcomings, and significant reputational harm. They also led local communities to believe that foreign partners tolerated corruption, thereby deepening resentment and eroding trust in the broader mission.

In either situation, you should not be the one to make the final recommendation on your own, lest suspicion later arise that it was a selfish rather than an impartial expert choice. Recognizing that such conflicts can arise, your military service will likely have regulations in place that would oblige you to disclose this potential conflict to your supervisors in the military and the government, who could then determine whether your advice was fully reliable and trustworthy.

When considering whether to hire PMSCs in military settings, states should carefully assess potential risks to security and the likelihood of violations of national and international law. Before contracting, they should evaluate whether their national legal framework is sufficient to prevent, investigate and remedy misconduct by PMSC personnel. When determining which activities to outsource, contracting states should ensure that PMSCs are not tasked with non-transferable state functions under IHL, such as directing participation in hostilities or overseeing internment sites. Furthermore, they should weigh carefully the degree of force and access to firearms granted to these companies. In high-risk or conflict-affected settings, these factors could heighten the risks of misconduct and violations of international law.

To mitigate such risks, contracting states must ensure that PMSCs conduct their activities in an ethical and responsible manner by exercising due diligence. Companies should not be selected solely based on cost, as lower costs often imply cutting corners and lowering professional standards. Instead, procurement processes should scrutinize companies' track records for integrity, reliability, and proven conformity with applicable national and international laws. Respect for international law should be embedded in all procurement and contracting practices.

MoD conflict-of-interest policies

Certain NATO countries have established COI policies within their defence ministries. For example, Canada's well-detailed directive, DAOD 7021-1, on Conflict of Interest and Post-Employment, applies to employees of the Department of National Defence (DND), while a related order sets principles for officers and non-commissioned members of the Canadian Armed Forces; both require the disclosure of potential conflicts through Confidential Reports (DND 2839-E).[43] The U.S. Department of Defence Standards of Conduct Office provides guidance on the prevention and disclosure of COI and enforces federal rules grounded in 18 U.S.C.§ 208.[44] In Germany, rules on dealing with cases of COI (*Interessenkollision*) apply to former members, civil servants, and soldiers of the Bundeswehr, particularly regarding secondary employment, and, depending on the category of person, different provisions of

43 National Defence, 'DAOD 7021-1, Conflict of Interest – Canada.ca', Canada.ca (2015), https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/7000-series/7021/7021-1-conflict-of-interest.html#pc; National Defence, 'Frequently Asked Questions – Conflict of Interest – Canada.ca', Canada.ca (2024), https://www.canada.ca/en/department-national-defence/services/benefits-military/defence-ethics/conflict-interest/frequently-asked-questions.html

44 Department of Defense Standards of Conduct Office, 'Conflicts of Interest', Osd.mil (2025), https://dodsoco.ogc.osd.mil/ETHICS-TOPICS/Conflicts-of-Interest

the Bundesbeamtengesetz (Federal Civil Servants Act) or Soldatengesetz (Act on the Legal Status of Military Personnel) apply.[45] The UK Ministry of Defence publishes a register of board members' private interests to promote public transparency;[46] and certain MoD agencies, such as Defence Equipment & Support (DE&S), use internal disclosure systems for staff.[47] In countries where no specific COI policy exists within the MoD, employees are generally subject to the broader ethics principles and COI provisions set out in national legislation.

Are conflicts of interest always immoral?

It is to be hoped not, because (unlike nepotism) they are difficult to avoid. A non-financial military example might be found once again on a promotion board, where a senior officer may be in a position to make decisions ostensibly about the career and promotion paths of other officers whose cases come before the promotion board. Unbeknown to others in the military hierarchy, those recommendations could affect that officer's own chances for promotion, or perhaps for obtaining a choice duty assignment for themselves. A COI simply arises whenever a person's official responsibilities intersect with circumstances that could influence, or appear to influence, their judgement. The example illustrates how a senior officer serving on a promotion board may evaluate candidates in ways that inadvertently affect their own future career prospects, such as influencing who becomes a future competitor or who may later serve as a superior. Even if the officer has no ill intent and acts impartially, the mere overlap between personal and institutional interests creates a COI. The key point is that the existence of a COI does not imply misconduct; moral concern arises only if the individual fails to recognize, disclose, or properly manage the situation.

What is clearly always wrong in these cases is for the person with the COI to continue to make the strategic decisions and to attempt to 'resolve' the inherent conflict alone. Experience in government, commerce, the military – just about everywhere a COI could be encountered – invariably reveals that the person with an often-glaring COI seems to be (or to appear to be) utterly unaware of it.

Dilemma: Beyond financial gain

A notable example of a COI dilemma extending beyond financial motives arose in connection with a government's consideration of whether to initiate an inquiry into the handling of detainees during an overseas military mission. Allegations had surfaced that detainees transferred to local authorities during the deployment were subjected to serious human rights violations, prompting a legal scholar and former legislator to submit a formal petition requesting an independent investigation. The petition was declined by the minister responsible for defence, who had previously served in the same mission at the time when the alleged mistreatment occurred. A subsequent complaint to the national ethics oversight body argued that the minister should have recused himself due to his prior involvement in intelligence and liaison activities related to the mission. The ethics authority ultimately concluded that the minister's past service did not constitute a 'private interest' under the relevant legislation and found no evidence of personal involvement in the detainee issue. However, the authority noted that the minister may have understated aspects of his earlier role, raising questions about the adequacy of disclosure.

45 Bundesministerium der Verteidigung, 'Interessenkollision', Bmvg.de (11 September 2025), https://www.bmvg.de/de/service/korruptionspraevention/interessenkollision

46 Ministry of Defence, 'Ministry of Defence Register of Board Members' Interests 2023 to 2024', GOV.UK (15 July 2024), https://www.gov.uk/government/publications/ministry-of-defence-register-of-board-members-interests-2023-to-2024

47 National Audit Office, 'Managing Conflicts of Interest' (November 2024), https://www.nao.org.uk/wp-content/uploads/2024/11/managing-conflicts-of-interest-good-practice-guide.pdf

Are conflicts of interest illegal?

COIs are difficult to identify and itemize in advance. Hence, they are difficult to capture in effective legislation. Instead, reliable and otherwise-trustworthy organizations, including military services, as we have seen, normally have regulations and policies in place requiring their members to disclose personal situations which might lead to a specific COI in advance of assuming duties and responsibilities.

Example: Uniform procurement

A significant procurement controversy emerged when a defence ministry contracted a private supplier to provide military uniforms that were later found to be substantially overpriced and of inadequate quality. Although the uniforms were documented as suitable for winter, they were, in fact, lighter, summer-weight items, and the contract had been awarded outside a standard open-tender procedure. Subsequent investigative reporting revealed that one of the company's co-owners was a close relative of a sitting member of the national legislature's defence committee. The legislator denied any connection to the contract or involvement in the company, and the relative later resigned from the firm. Reports also indicated that the same individual purchased high-value real estate shortly after stepping down, though attempts by journalists to obtain comment were unsuccessful. The case illustrates how undisclosed personal relationships in procurement processes can create the appearance of a COI, even in the absence of proven illegality. It also underscores the broader need for clear procedures, requiring defence personnel and decision-makers to identify, report, and mitigate actual or potential COIs in order to preserve institutional integrity.

Revolving-door controversies

Another common COI risk is the so-called revolving-door phenomenon, in which individuals move between public sector roles and private sector positions. Although not inherently unlawful, such transitions can become ethically sensitive when former officials assume roles in industries affected by decisions they previously oversaw, or when private sector experts enter public office and their former employers later benefit from government contracts.

In one instance, a former senior government official accepted a high-level lobbying position with a major defence manufacturer shortly after leaving public service, prompting public concern that past regulatory responsibilities could create the appearance of undue influence. In a reverse scenario, an individual who had previously served as a partner at a consulting firm was appointed to a top leadership role in a defence ministry, after which the consulting firm reportedly secured significant advisory work with that ministry. Although the official denied involvement in the selection of those contracts, the situation raised broader questions about transparency, impartiality, and the adequacy of safeguards governing potential COIs in public procurement.

Are conflicts of interest moral dilemmas or tests of integrity?

They can be moral dilemmas or tests of integrity, or both, depending upon circumstances. But most often, and certainly in all three examples already shown here, they are tests of integrity. A well-intentioned military professional will surely recognize, in the military cases outlined, that when such conflicts arise, they are facing a severe test of their integrity. Passing the integrity test will require the person facing questionable choices to seek outside help in resolving them, as well as complying fully with procedures and regulations requiring disclosure of actual (and potential) COIs, in order to maintain the reputation of their service and the profession itself.

To prevent COIs (or even the prospect of COIs) from bringing about harm ranging from incompetence to outright corruption and abuse of power, it is important for military services to have in place a policy or regulation that requires disclosure of factors (e.g. financial interests) that could skew decision-making or cast doubt upon the reliability and integrity of the decisions made or policies enacted. COIs (or even the possibility of COIs) of any form sow suspicion and mistrust among the rank and file of any organization. Allowing them to persist unchallenged clouds public trust in the decisions and policies thereby enacted.

Transparency measures such as mandatory declaration of interests, regular reporting, and robust internal disclosure systems form a crucial foundation for preventing and managing COI. These tools must be supported by dedicated monitoring bodies within ministries and across government, empowered to verify disclosures, investigate concerns, and provide guidance on mitigation.

Remember that

- ✓ COIs arise when personal interests affect – or appear to affect – impartial duty.
- ✓ Even perceived COIs erode trust and credibility.
- ✓ Systemic risks (e.g., revolving doors and lobbying) need strong safeguards.
- ✓ Prevention tools: disclosure, recusal, independent review, and training.
- ✓ Accountability must span laws, oversight bodies, and ethical culture.

Check-your-skills exercises

Task 1. COI analysis and guided discussion

The facilitator will present each case and ask the guiding questions directly to the audience to encourage active participation. Participants will be prompted to analyse the situation, identify risks, and propose solutions before moving on to the model answers. This interactive questioning ensures the participants apply the concepts to practical scenarios and develop critical thinking skills around COI management.

Activity 1: Definition and scope of COI

Case: A senior procurement officer is evaluating bids from various companies, one of which is partially owned by their cousin.

Model answer: This is an actual COI because a close family relationship could directly influence the decision-making process. The officer should immediately disclose the relationship and recuse themselves from the evaluation.

Guiding questions:

- How would this change if the cousin's company withdrew before final selection?
- What if the officer had no knowledge of the cousin's ownership?

Debriefing notes: Clarify the distinction between actual, perceived, and potential COIs. Stress that even without wrongdoing, the appearance of bias can damage institutional credibility.

Activity 2: COI in defence and military contexts

Case: A base commander approves overtime for a logistics company that employs his spouse.

Model answer: This is an actual COI with operational implications. There is risk of resource misallocation and perceived favouritism, affecting morale and trust. The commander should have disclosed the relationship and delegated the decision.

Guiding questions:

- How does the amount of pay influence the seriousness of the COI?
- Would the risk be lower if the spouse had a non-influential position in the company?

Debriefing notes: Highlight that COIs can arise at any level of decision-making, not just senior ranks. Link this to operational integrity and fairness.

Activity 3: Structural COI risks

Case: A defence minister accepts employment at an arms manufacturer after leaving office.

Model answer: This is a systemic risk from the revolving-door phenomenon; it could lead to 'policy capture' and undermine public trust; possible safeguards are cooling-off periods and restrictions on lobbying.

Guiding questions:

- How long should the cooling-off period last for?
- How do we balance preventing COIs with allowing post-service careers?

Debriefing notes: Encourage participants to think about institutional safeguards and to share examples from their own country.

Activity 4: Preventative and disclosure mechanisms

Case: An officer fails to disclose that their sibling owns a cybersecurity firm bidding for a defence contract.

Model answer: Failure to disclose undermines transparency and can invalidate procurement decisions. Disclosure policies and enforcement mechanisms are critical.

Guiding questions:

- Should failure to disclose always result in disciplinary action?
- What systems help ensure disclosures are accurate and updated?

Debriefing notes: Link to accountability culture – policies are only effective if supported by enforcement and ethics training.

3.6. Truth versus loyalty: Whistle-blowing

Module objectives

Participants will explore the ethical dilemmas surrounding whistle-blowing in military and professional contexts. They will analyse the conflict between truth and loyalty, distinguish between internal and external whistle-blowing, and evaluate real-world cases to understand when whistle-blowing is ethically justifiable. The training aims to strengthen the participants' ability to balance loyalty, justice, and professional responsibility when facing misconduct or harmful practices.

Key information

a. The ethical dilemma of truth versus loyalty. Whistle-blowing highlights the conflict between fairness (justice, impartiality, public interest) and loyalty (to commanders, colleagues, or the organization). Soldiers face competing obligations: protecting their 'fellows' versus safeguarding broader public safety and justice.

b. Internal vs external whistle-blowing. Internal whistle-blowing occurs when wrongdoing is reported within the chain of command. External whistle-blowing occurs when information is taken outside the organization (e.g. to the press, public, or law enforcement). External whistle-blowing is only ethically defensible as a last resort.

c. Criteria for ethical whistle-blowing. Ethical whistle-blowing generally requires:

- Clear evidence of serious and imminent harm to the public
- Proportionality (the harm prevented must outweigh the harm caused by disclosure)
- Exhaustion of internal reporting channels, unless waiting would worsen the harm
- Right intention (to serve the public good, not personal revenge or gain).

d. Layers of loyalty in military service. Loyalty is not unlimited. Soldiers owe loyalty to their fellow soldiers, their chain of command, their country, and their citizens. When misconduct occurs, loyalty to the public interest may override loyalty to individuals or immediate superiors.

e. Risks and consequences for whistle-blowers. Whistle-blowers often face retaliation, professional isolation, or legal consequences, despite acting out of moral courage. Cases like that of Libor Michalek (see the next section) show that whistle-blowing can carry heavy personal costs, even when ultimately vindicated.

f. The professional duty of moral courage. Military professionalism requires both loyalty and integrity. Whistle-blowing, when undertaken responsibly, can uphold institutional values and protect public trust. Soldiers must cultivate moral courage to confront wrongdoing, even at personal risk, while respecting confidentiality and national security concerns.

Module content

Stories of whistle-blowers have formed the plotlines of many Hollywood films; they are invariably glamourized in these portrayals. In the real world, the whistle-blower does not always win praise or glory for their moral courage; it is often the opposite – the whistle-blower is punished or reviled. Consider the example of the Czech economist and politician Libor Michalek, who twice blew the whistle on corruption within the Czech government.[48] First, Michalek uncovered a huge embezzlement scheme; after reporting it, Michalek was fired for 'gross violation of labour discipline'. It took him a year in court to get his job back. Later, while working at another agency, the State Environmental Fund, he uncovered one of the biggest scandals in Czech history, involving the environmental minister, the head of police, and numerous other government officials. As the corruption scandal unfolded, politicians tried to discredit him both privately and professionally, and Michalek and his family received so many threats they had to be placed under police protection. In light of these examples, potential whistle-blowers may be wise to consider reporting anonymously. Many countries now have electronic mechanisms for whistle-blowing to protect the whistle-blower's anonymity, as well as laws to protect the whistle-blower against retaliation.[49] But while Libor Michalek was unable to remain anonymous, his story eventually showed how much his crusade was valued by the public at large. Michalek was nominated for the Czech senate in the 2012 elections. His reputation as a fighter against corruption helped him win 75 per cent of the votes.

Consider the situation in which a service member receives an order from a superior that appears unethical or unlawful. While obedience to command is a fundamental duty, it does not extend to carrying out actions that are clearly improper. In such circumstances, a service member must determine the appropriate course of action: raising the concern with the issuing commander, reporting the matter to a higher authority within the chain of command, or in exceptional cases alerting external bodies such as law enforcement agencies or the press. Similarly, one should reflect on the appropriate response when witnessing misconduct or corruption within the organization. As a service member, you may be privy to sensitive information, and you know that you have a responsibility to keep military matters confidential. But if you see someone within the organization acting in a way that is improper, perhaps you also have a responsibility to the public. What should you do? These sorts of dilemmas fall into the category we call whistle-blowing.

The English term 'whistle-blower' seems to have originated from the 19th-century police in the US and UK, who blew whistles to alert the public or fellow police of a crime taking place. It now means someone within an organization who attempts to draw their superior's attention to something unethical or illegal. If the superior does not address the wrongdoing, the whistle-blower may feel compelled to circumvent the normal chain of command and report the wrongdoing to a higher authority within the organization. Recently, the word has been adopted as the name for someone who is trying to alert others to wrongdoing inside their organization by going outside of the organization and revealing information about the wrongdoing to the public or to members of the press. Going public with information about wrongdoing that is taking place within an organization is called *external* whistle-blowing. It is meant as a positive-sounding alternative to names such as informer, snitch, tattler, or leaker (in English), which have negative connotations.

Is whistle-blowing an act of heroism or betrayal? The person who blows the whistle by reporting outside his organization apparently believes that the public interest overrides the interest of the organization that they serve. But some would argue that a person's primary duty is that of loyalty to the organization, or loyalty to those with whom they have a personal relationship. In fact, reporting someone's unethical behaviour to a third party often constitutes a moral dilemma, a conflict between competing moral concerns. The conflict is

48 See https://www.occrp.org/en/victimsofcorruption/tempted-to-steal-be-afraid-of-libor-michalek

49 See, for example, https://idfi.ge/en/whistleblower_institute_in_georgia_

between two specific moral values: fairness (or justice) and loyalty. At its core, the value of fairness (or justice) demands *impartiality*: all persons and groups must be treated equally. It is clearly unjust or unfair if members of the public are being exploited and those within the organization are profiting at their expense. By contrast, the value of loyalty dictates *preferential treatment*, a responsibility to favour one's own group over other groups, and people close to us over people with whom we do not have a special relationship. But which of these should take precedence?

A soldier witnesses someone violating procedures, falsifying data, or failing to tell the whole truth. Should they report to those in command? If this person is a 'brother in arms', one probably feels a bond of loyalty to them. Bonds of loyalty are sacred within a military organization, since the fate and well-being of each soldier is bound up with every other soldier. Each member of the military is asked to take extra risks and bear special burdens for their fellow soldiers, and soldiers have often claimed that in battlefield situations their will to fight comes from wanting to protect the soldiers fighting alongside them, as opposed to devotion to some abstract principle such as freedom or love of country. So loyalty among what Shakespeare called a 'band of brothers' is precious, and must be recognized as a moral virtue. Nevertheless, loyalty should not be unlimited. If loyalty conflicts with other moral principles, or if being loyal to someone means betraying your own core beliefs or principles, it is important to reassess whether your loyalties are misplaced. There are, in fact, layers of loyalty which may be in conflict and which the soldier must untangle. Military service certainly involves loyalty to one's *country* and one's *fellow citizens*, in addition to one's *fellow soldiers*. If a fellow soldier has violated procedures, falsified data, or failed to tell the truth, they may no longer be worthy of your loyalty; they have forfeited their claim to it. Your country and your countrymen, however, still make a claim on your loyalty. By way of this larger loyalty to a greater community, we see that our moral values do not conflict.

If corruption is endemic in a culture or in an organization, external whistle-blowing may be the most effective way to put a stop to it. Practically speaking, however, wrongdoing within an organization should first be addressed at the lowest possible level – confront a fellow soldier who has done something wrong, rather than report them, and if a problem remains, report it at the lowest levels in the chain of command. Going public with your observations of wrongdoing should be a last resort. Only if you fail to get the responsible person in your chain of command (e.g. your highest-ranking officer, or inspector general) to take action first, would it be morally justifiable to go public. Even then, the issue must be sufficiently serious to outweigh the disruption and harm that going public inevitably causes.

Dilemma: Should militaries inform the media?

A notable whistle-blowing case arose when a fleet of advanced military aircraft was grounded for several months after multiple incidents in which pilots experienced a dangerous lack of breathable oxygen, leading in one instance to a fatal crash. Despite an ongoing technical investigation, the fleet was cleared to resume flying before the root cause had been identified. Although interim safety measures were introduced, additional incidents continued to occur, leaving some pilots convinced that the aircraft posed unacceptable risks to both aircrew and people on the ground.

Two pilots who had personally experienced near-loss of consciousness during training flights raised concerns through official channels but were dissatisfied with the response, which characterized the remaining risk as acceptable. One was temporarily excused from flying but was warned that refusal to return to duty could jeopardize their career, while the other was formally reprimanded and faced financial penalties. Believing that internal mechanisms had failed to address a serious safety hazard, both pilots ultimately chose to disclose their concerns publicly through a media outlet, effectively bypassing the usual chain-of-command processes.

This situation raises a central ethical question: whether personnel in such circumstances are justified in going outside formal reporting structures to protect lives, or whether concerns should remain within established military channels even when those channels appear unresponsive.

- The first thing a potential whistle-blower should consider is the status of the information itself. Is the information 'classified', 'proprietary', or otherwise 'protected'? Is there a system in place which clearly considers this information restricted? If the information is clearly intended to be protected, then the whistle-blower must have substantiated reason for leaking it.
- The second consideration is whether the potential whistle-blower has a specific obligation, legal or ethical, to protect the information, or is in possession of the information only because another person has violated their obligation to keep it secret. If so, then it is a much more serious matter to reveal it.
- The third consideration is whether the information concerns public or private matters. Information about another's sexual orientation, about their private finances, or about personal phone calls has more of a claim to privacy than information about a person's actions as a corporate executive or a government official. The difficult cases, of course, are those where the private life of an individual arguably influences their public actions.
- The whistle-blower must determine if the conduct they are exposing represents actual wrongdoing or if it simply represents a policy disagreement. Those in command may have strong disagreements with one another, but these should remain classified if the problem does not rise to the level of misconduct.

You can read more about this topic here: K. O. Hanson and J. Ceppos, 'The Ethics of Leaks'. Markkula Center for Applied Ethics, Santa Clara University. Available at: https://www.scu.edu/ethics/focus-areas/journalism-and-media-ethics/resources/the-ethics-of-leaks (Accessed 24 November 2025).

Ethical whistle-blowing

A widely discussed whistle-blowing case involved an intelligence-sector contractor who disclosed classified information to major international media outlets. The individual stated that the sole motivation for releasing the material was to inform the public about surveillance practices carried out in their name and, in their view, against their interests.

Supporters argued that the situation met one common criterion for ethical whistle-blowing: that significant harm to the public must be at stake. Although no physical harm had occurred, the whistle-blower claimed that the surveillance practices posed psychological risks and threatened broader civil liberties. They also emphasized an obligation to uphold constitutional principles that prohibit sweeping, pervasive monitoring of citizens.

Another standard criterion for ethical whistle-blowing is that it should occur only as a last resort. The whistle-blower asserted that concerns were first raised with immediate supervisors, though it remains unclear whether the issue was pursued further up the internal hierarchy. Advocates have argued that additional escalation may not have been feasible or safe, given the sensitive nature of the disclosures and perceived limitations of internal reporting mechanisms.

Remember that

- Whistle-blowing balances truth and fairness against loyalty.
- Internal reporting is preferred – external disclosure is a last resort.
- Ethical whistle-blowing needs evidence, proportionality, proper intent, and use of internal channels.
- Loyalty to public interest can outweigh loyalty to individuals.
- Whistle-blowers face risks and need moral courage to act.
- Responsible whistle-blowing protects values, trust, and professionalism.

Check-your-skills exercises

Task 1. Case study: Whistle-blowing during a shipboard health crisis

A high-profile whistle-blowing incident occurred when the commanding officer of a large naval vessel faced a rapidly escalating outbreak of a contagious illness on board. Standard containment measures of removing infected personnel, isolating close contacts, and attempting to stop transmission became ineffective due to the close quarters of ship life, where nearly everyone had been exposed. Concerned that the situation posed immediate and severe risks to the crew, the commanding officer sent an urgent message to senior leadership requesting stronger intervention. The message was distributed to several senior officers beyond the individual's direct chain of command and was later leaked to the media, prompting widespread attention. Shortly afterwards, the officer was removed from command, effectively ending a long naval career.

Activity:

Participants should be divided into four groups, each addressing one of the following ethical questions:

- When is it ethical to act outside the chain of command?
- When is it morally right to violate confidentiality obligations?
- When, if ever, is it acceptable to disclose military activities to the press?
- How do the following criteria apply to this case?

Ethical whistle-blowing may be justified only if:

- There is a significant and imminent threat to the public
- The harm prevented outweighs the harm caused by whistle-blowing
- All reasonable internal avenues have been exhausted
- The motivation is to serve the public interest.

Facilitator notes:

1. It is unclear whether this incident constitutes true external whistle-blowing. Although leadership alleged that the commanding officer leaked the information publicly, definitive proof is lacking. The message was, however, sent to multiple senior leaders outside the immediate reporting line.
2. The officer's actions appear broadly consistent with ethical whistle-blowing principles:
   - The concern involved a significant and growing risk to personnel, and intentions seem aligned with protecting lives.
   - Determining whether the 'last resort' criterion is met is difficult, as one can always attempt further internal appeals.
   - Given the rapid spread of illness and the dangers of delay, it can be argued that the urgency justified going outside the normal chain.
   - Although the severity of the illness was not fully understood at the time, the potential harm being averted arguably outweighed the risks of broader disclosure.
3. The ethical ambiguity lies in whether sending the message to ten senior officers – later leaked to the media – was appropriate:
   - If the aim was to maintain deniability while publicly pressuring leadership, the approach might be viewed as tactically questionable.
   - It remains unclear which internal channels had already been attempted or exhausted.
4. Although the officer was relieved of command for bypassing procedure and allegedly mishandling the situation, the ethical assessment is more nuanced:
   - Senior leaders later argued that the message created unnecessary alarm.
   - Regional command authorities claimed that evacuation and mitigation plans were already underway and that the disclosure complicated logistical negotiations.
   - It may also be argued that clearer communication from higher leadership could have prevented the misunderstanding and the perceived need to escalate concerns externally.

3.7. Ethical dilemmas during combat operations

Module objectives

Participants will understand the types of ethical dilemmas that arise during combat operations, evaluate them through the lens of IHL, and critically reflect on the balance between military necessity, professional conduct, and humanitarian principles.

Key information

a. Balancing military necessity and humanitarian values. Combat operations often force commanders and soldiers to weigh immediate tactical objectives against the principles of IHL. Distinguishing between combatants and civilians, applying proportional force, and preventing collateral damage are central to this dilemma.

b. Humane treatment of detainees and prisoners of war. Captured combatants and civilians caught in conflict are entitled to humane treatment under the Geneva Conventions. Torture, summary executions, or cruel treatment not only violate international law but also undermine professional military ethics and long-term strategic objectives.

c. Legal frameworks that constrain warfare. IHL regulates both the conduct of hostilities and the protection of persons. While earlier Hague law focused on means and methods of warfare and Geneva law on protected persons, contemporary IHL – particularly through Additional Protocol I to the Geneva Conventions – integrates both functions.

d. Obedience to orders versus moral responsibility. Military personnel are obliged to follow lawful orders but also have a duty to disobey manifestly illegal ones. This creates ethical tension, as loyalty and discipline may conflict with conscience and the legal duty to prevent war crimes.

e. Lessons from atrocities and case studies. Incidents such as in Bucha, Ukraine illustrate how ethical failures in combat result in profound humanitarian suffering, moral injury among soldiers, and loss of legitimacy for the armed forces.

f. The importance of ethics for soldiers and societies. Upholding ethical standards in combat not only protects civilians and supports the principles of humanitarianism but also shields soldiers from moral injury, sustains public trust in the armed forces, and preserves the foundations for peace after conflict ends.

Module content

Combat operations raise complex ethical dilemmas that often revolve around balancing military necessity with humanitarian principles. One recurring challenge is distinguishing combatants from civilians, especially when adversaries operate within populated areas, which complicates the proportional use of force and heightens the risk of collateral damage. The use of lethal force also presents questions of whether to kill or capture enemy combatants, as rules of engagement may constrain action to protect non-combatants. The treatment of detainees and POWS tests adherence to humane standards, particularly when under pressure during interrogations. Protecting cultural sites and civilian infrastructure poses another dilemma, as their destruction may yield tactical advantages but carry long-term humanitarian and moral costs.

Technological developments introduce new challenges, such as the deployment of autonomous or remotely piloted weapons, which distance decision-makers from the battlefield and blur lines of accountability. At the same time, soldiers face conflict between obeying orders or maintaining moral responsibility when confronted with potentially illegal directives. Gathering intelligence through civilian cooperation also raises ethical concerns, as it can expose vulnerable populations to danger, while the use of psychological operations stretches the boundaries of acceptable influence. Medical neutrality adds further complexity, requiring difficult decisions about prioritizing care for friendly forces, enemy combatants, or civilians.

The use of child soldiers and other vulnerable groups as combatants tests the limits of engagement rules, while the overarching principles of proportionality and necessity force militaries to weigh immediate operational gains against broader humanitarian consequences. Ultimately, these dilemmas underscore the constant conflict between what is legally permissible under IHL and what is morally defensible in the conduct of war.

The Law of Armed Conflict (LOAC) is a set of rules and principles governing the behaviour of combatants during war. The principles are embodied in a series of treaty agreements, or Conventions, adopted over the past century by international bodies of state representatives, meeting in European cities such as The Hague and Geneva (and named accordingly).

The Hague Conventions primarily govern means and methods of warfare, conduct of hostilities, and occupation. That is, they tend to focus on the proper conduct of armed hostilities by opposing military forces. Their provisions place limits on the amount of force used in specific combat operations, and prohibit the use of certain kinds of weapons. Force is only to be used to achieve legitimate and reasonable military objectives (‘military necessity’), and only as much as is required to attain those objectives (‘proportionality’).

So, if a village housed a group of insurgents, it might be deemed necessary from a military standpoint to capture the village and kill or imprison the insurgents. But it would not be reasonable to firebomb the entire village. It would certainly not be reasonable to use a nuclear weapon to achieve this military objective. Such a use of force would almost certainly be deemed ‘excessive’: i.e. way more than necessary, and all out of proportion’ to the significance of the military’s purpose in capturing the village.

In addition, the use of certain prohibited weapons, such as poison gas or exploding bullets, has been found to inflict ‘superfluous injuries’ or cause cruel and unnecessary suffering, neither of which furthers the legitimate military objective. Poison gas and nuclear weapons, moreover, are examples of ‘weapons of mass destruction’ (WMDs) which fail to distinguish between enemy combatants and civilian non-combatants, and so are also prohibited on those grounds. The Hague Conventions thus primarily address the weapons and tactics of warfare itself, as practised between opposing military forces, and constitute the LOAC.

The Geneva Conventions primarily provide protection to war victims. They are written declarations resulting from assemblies usually convened by the International Committee of the Red Cross (ICRC), headquartered in Geneva. These deliberations approach the problem of war from the standpoint of people inevitably caught between opposing armies: i.e. refugees, civilian non-combatants, and POWs. These conventions attempt to define and establish certain rights and protections to be afforded those victims (such as not being deliberately subject to attack by competing militaries). They also afford recognition and protection to medical personnel attempting to render aid to these victims.

By affording specific rights and protections to each of these groups, the Geneva Conventions require that military personnel recognize the special and protected status of such people caught in the midst of hostilities. This fundamental principle goes by many equivalent names: the so-called principle of distinction (in law) or of non-combatant immunity, which is also called the Principle of Discrimination. These conventions (plus some customary protocols and precepts) are referred to collectively as international humanitarian law or IHL. Here are some specific examples of IHL:

- Those not posing a threat in combat must be treated humanely.
- It is forbidden to harm an enemy who is surrendering.
- No one may be subjected to torture.
- Civilians may not be targeted.
- Captured combatants must be treated humanely, cared for if injured, and allowed to correspond with their families.

Battlefield dilemmas

One factor that distinguishes a combatant from a common murderer is that killing, or the exercise of deadly force, is always undertaken discriminately, proportionately, and only when *absolutely necessary to defend the state and fellow citizens from harm*. Killing unarmed and defenceless POWs – persons rendered *hors de combat* – is, by contrast, strictly prohibited. We might wonder what other principles make up this code, and in our remaining sessions, we will try to identify them. By recognizing this as a *self-imposed moral code* for members of the profession of arms themselves, we thereby distinguish these moral constraints on war from the strictures of international law.

Watch the video about a Ukrainian military medic who helps a Russian prisoner of war: Ukrainian Soldier Treats Russian POW During Capture

A core historic document (the Lieber Code) is often cited when discussing the origins of modern IHL. Its formal name is General Orders 100, and it was initially drafted by a committee of senior military officers during the mid-19th century. The committee's leader was a former Prussian military officer who had fought in the Napoleonic wars and subsequently come to the US to practise law.

At the behest of President Abraham Lincoln, this German-American soldier and jurist, Hans Lieber, convened a working group of military personnel to draft a series of 'Standing Orders' for US (Union) military during the American Civil War. These Orders specifically required that military personnel in the Union Army refrain from torturing or killing captured POWs from the rebel army. Apart from that, military personnel were required at all times to behave honourably and with integrity, to treat non-combatants from both sides of the conflict with dignity and respect, and to refrain from excessive or unnecessary use of force.

This new document was universally admired, and the code of conduct it established was widely adopted, first by the Prussian Army, and subsequently by virtually all standing armies in Europe. It set forth, for the first time, in written form, the principles of military necessity, proportionality, command responsibility, and proper treatment of enemy prisoners that together define this 'Code of the Warrior'.

Dilemma 1: An enemy soldier has killed your brother during combat and is now surrendering. What should you do?

You are engaged in combat, fighting side by side with your brother. In the heat of battle, an enemy soldier kills him. Moments later, that same enemy lays down his weapon and attempts to surrender. You are suddenly confronted with a profound conflict between personal grief and professional duty. On the one hand, your emotions push you towards anger and revenge; on the other hand, your role as a soldier obliges you to act in accordance with the LOAC and the ethical standards of military service.

The professional and legal course of action is to accept the surrender and take the enemy soldier as a prisoner of war. This preserves discipline, upholds IHL, and ensures that your conduct remains above reproach. Yet, this path is not easy. Allowing the man who killed your brother to live may feel deeply unjust, and the temptation to reject his surrender is powerful. Acting on this impulse, however, would constitute a war crime, undermine the moral authority of your unit, and compromise your integrity as a soldier.

Another option is to step back and transfer responsibility for handling the surrender to another member of your unit or a superior officer. This allows you to remove yourself from a situation where grief and anger cloud your judgement, while still ensuring that the rules of war are respected. In doing so, you acknowledge your emotional state without betraying your ethical and legal obligations.

This dilemma highlights the painful conflict between personal loss and professional responsibility. It forces reflection on what it means to be a soldier: to endure sacrifice, to master emotions, and to act not only as an individual but as a representative of your nation and its values. Ultimately, the decision you make will resonate far beyond the battlefield, shaping the trust within your unit, the legitimacy of your cause, and your own moral character.

Dilemma 2: During combat operations, do you sacrifice the civilian population or your own unit?

During combat operations, a devastating dilemma may arise: whether to risk the safety of the civilian population or to protect your own unit. On the battlefield, circumstances can force leaders to make choices under immense pressure, where every decision carries irreversible consequences.

The lives of non-combatants may depend on restraint, patience, and the willingness to accept losses within one's own ranks. At the same time, every commander carries the responsibility to safeguard their soldiers, who have placed their trust and survival in their leader's hands.

Sacrificing civilians in order to preserve the unit might offer a tactical advantage or protect the immediate fighting force, but it comes at an unbearable ethical cost. Such an action would violate IHL, erode the legitimacy of the mission, and undermine the very values the armed forces are sworn to defend. Conversely, prioritizing civilian lives over those of one's own soldiers demonstrates moral courage and respect for the laws of war, but it also means accepting the possibility of significant military losses, which could weaken the unit's effectiveness and morale.

This dilemma illustrates the harsh reality of modern warfare, where ethical principles, legal frameworks, and human emotions collide in moments of crisis. Leaders must weigh their obligations: the duty to protect their soldiers, the duty to safeguard civilians, and the duty to uphold the moral standards of their nation and military profession. No choice is without pain, but the way such decisions are made defines not only the outcome of a battle but also the moral integrity of the forces engaged in it.

Dilemma 3: During combat, you are confronted by a child soldier pointing a weapon at you. How should you respond?

In the midst of combat, you suddenly face a child soldier pointing a weapon directly at you. The child is clearly armed and poses a real and immediate threat to your life and the lives of your comrades. At the same time, you are aware that this is not a typical enemy combatant but a minor – someone who may have been coerced, manipulated, or forced into fighting. The decision you make in the next few seconds will have both tactical and ethical consequences.

You are torn between two conflicting duties: the obligation to protect yourself and your unit, and the obligation to safeguard children, who are legally and morally recognized as vulnerable individuals, even in war.

The professional and ethical response is to treat the child soldier as both a threat and a victim. If the child is actively aiming a weapon at you and preparing to fire, the LOAC permits you to defend yourself, even with lethal force if there is no other option. However, if circumstances allow, you should try to neutralize the threat without killing the child – for example, by disarming, capturing, or incapacitating them.

In practical terms, this might mean using non-lethal force where possible, seeking cover while attempting to de-escalate the situation, or coordinating with your unit to overpower the child without resorting to lethal action. Once disarmed, the child must be treated humanely, in accordance with IHL, recognizing that they are primarily a victim of exploitation rather than a willing enemy.

This dilemma underscores the brutal complexity of modern conflict, where children are sometimes forced into combat roles. Soldiers must balance their right to self-defence with their duty to uphold ethical and legal standards. While survival may demand immediate defensive action, the long-term responsibility is to protect children from further harm and to ensure that they are treated not as criminals, but as victims in need of care and rehabilitation.

Dilemma 4: Use of torture or coercive interrogation?

During combat operations, your unit captures an enemy fighter believed to possess crucial intelligence about an imminent attack on a civilian target – perhaps a hospital, a school, or a residential area. The attack could cause mass casualties if it is not prevented. Time is short, and conventional intelligence channels may not deliver answers fast enough.

Faced with this urgency, you are confronted with a moral and legal dilemma: should you use torture or coercive interrogation methods to extract the information? On the one hand, doing so could potentially save innocent lives. On the other hand, it would involve violating international law, professional codes of conduct, and fundamental human rights. What are the possible solutions?

A decision to inflict pain or severe psychological pressure might be justified under the logic of ‘the greater good’. However, this course of action is unlawful under the Geneva Conventions, the UN Convention Against Torture, and most military codes. It carries serious long-term consequences: undermining the legitimacy of your mission, eroding moral authority, and potentially radicalizing more enemies. Furthermore, evidence shows that torture often produces unreliable information, as individuals under extreme duress will say anything to stop the suffering.

One could pursue ethical and legal questioning methods, using rapport-building, psychological pressure, and lawful techniques designed to elicit cooperation. This option maintains compliance with IHL and preserves the moral high ground. While it may take longer and the risk of civilian casualties remains, it protects the integrity of the armed forces and prevents future accountability issues.

Instead of acting alone, one could immediately inform higher command and intelligence agencies, ensuring the decision is made collectively within legal and ethical frameworks. This distributes responsibility, allows for broader use of intelligence-gathering resources, and ensures transparency.

This dilemma forces leaders to weigh utilitarian arguments – sacrificing one for many – against the principles of law, morality, and professional ethics. While the instinct to save lives at any cost is powerful, crossing the line into torture erodes the very values soldiers are sworn to defend. Upholding ethical standards, even under extreme pressure, ensures that the armed forces remain credible and disciplined.

The use of private military and security companies

Across the world, governments are increasingly turning to PMSCs to address not only limitations in resources, expertise, or manpower, but also growing levels of conflict and insecurity. As a result, PMSCs are increasingly serving in roles previously performed only by national armed forces, such as supporting military operations with logistics, intelligence, or training. In some cases, they might even engage in combat. Despite the benefits offered by private security services, this trend towards the privatization of force raises serious concerns about accountability, transparency, and the risk of abuse.

While these companies can provide valuable services, it is important to remember that PMSCs are profit-driven enterprises and their personnel are rarely held to the same ethical standards as members of armed forces. Moreover, operating in areas marked by weak governance, active conflict, and limited state oversight can create an environment highly conducive to abuse and misconduct. A lack of transparency in business structure and/or unclear chains of command can further challenge traditional military hierarchy and create accountability gaps for IHL violations. States must therefore carefully weigh the moral and legal implications of employing PMSCs in military operations or other defence contexts.

The 2021 indiscriminate attacks committed by Dyck Advisory Group in Mozambique

In 2021, the Mozambican government hired the South African private military company Dyck Advisory Group (DAG) to fight the Al-Shabaab insurgency on its behalf using armed helicopters. With little to no state oversight, the firm directly participated in hostilities, committing serious violations of IHL and fuelling further conflict in the Cabo Delgado region. According to an Amnesty International report, DAG operatives fired machine guns from helicopters and dropped hand grenades indiscriminately into crowds of people, as well as repeatedly firing at civilian infrastructure, including hospitals, schools, and homes.[50] The Mozambican government has yet to address these allegations or hold the company accountable.[51]

50 Amnesty International, 'Mozambique: Civilians killed as war crimes committed by armed group, government forces, and private military contractors – new report' (2 March 2021), https://www.amnesty.org/en/latest/news/2021/03/mozambique-civilians-killed-as-war-crimes-committed-by-armed-group-government-forces-and-private-military-contractors-new-report

51 Business & Human Rights Resource Centre, 'Mozambique: Private military company to investigate allegations that is killing civilians in Cabo Delgado conflict' (4 March 2021), https://www.business-humanrights.org/en/latest-news/mozambique-private-military-company-to-investigate-allegations-that-is-killing-civilians-in-cabo-delgado-conflict

In addition, misconduct by PMSC personnel can pose serious reputational risks for contracting states. Associating with firms implicated in human rights abuse, war crimes, and other breaches of international law can undermine the legitimacy and credibility of defence institutions, especially if incriminated PMSCs have been integrated into regular armed forces or operate under direct military command. Because the provision of security is a core state function, PMSCs perceived as uncontrolled can also weaken overall public trust in the state.

While international law does not endorse or prohibit the use of PMSCs in defence contexts, states are obliged to prevent and address any harm resulting from their actions. As private actors, PMSCs are not directly bound by international law.

Remember that

- ✓ Combat demands balancing military necessity with humanitarian principles.
- ✓ Detainees and POWs must be treated humanely – torture violates law and ethics.
- ✓ Soldiers must follow lawful orders and refuse illegal ones.
- ✓ Atrocities show how ethical failure harms civilians, forces, and legitimacy.
- ✓ Ethical conduct protects civilians, soldiers, public trust, and post-war peace.

Check-your-skills exercises

Task 1. Are there any rules or constraints that limit our conduct during armed conflict? Discuss the example.

Instructions:

- Divide participants into two groups.
- Assign the case to each group.
- Allow 15 minutes for small-group discussion
- Then allow the groups 5–7 minutes each (15 minutes in total) to report back to the whole class.

Case-study:

Mass killings of civilians and detained persons have been documented in a town where hundreds of bodies were recovered following the withdrawal of occupying forces. Local authorities have reported hundreds of deceased individuals, including several minors. Most victims show signs of having been killed with weapons, while others appear to have died while held in captivity. Independent international monitors have confirmed numerous 'unlawful killings', including summary executions. Photographic evidence has revealed bodies discovered in a basement, many with hands bound and bearing close-range gunshot wounds. Additional reports have described mutilation, the burning of bodies, and sexual violence against minors. Intercepted communications indicate that the operations, which involved identifying, detaining, torturing, and executing targeted individuals, were referred to by the perpetrators as a form of 'cleansing'.

Questions for small-group discussion:

- This is war. It is violent and brutal. Innocent people die just like enemy combatants do. Are these specific actions simply a part of that unfortunate tragedy? If not, what is the difference?
- Absent the wartime setting, such actions would without question be classified as atrocities and mass murders. Apparently, the killings are not random, accidental, or unintentional. They are deliberate actions. Does this mean that 'soldiers' are simply murderers for hire who wear their nation's uniforms?

Instructor: 'Let us try now to look at the question of supposed rules and laws regulating warfare from the perspective of those who wear the uniform and employ deadly force to protect their country and fellow citizens from harm. Suppose you and your fellow combatants had blanket immunity from prosecution under international law. That is, no one would try to indict or punish you for your activities in combat.

'Given your apparent freedom to act without reprisals, what would you do in any of the following situations? And how would you and your fellow soldiers feel about your actions afterwards?'

Instructions:

- Divide your class into three small discussion groups (with different members this time).
- Allow 15 minutes to discuss the following situations.
- Then allow the groups 10 minutes each (30 minutes in total) to report their decision to the whole class.

You find yourself depressed, drunk, angry, upset, sleep-deprived for days, and tired of combat deployment. In a fit of rage one sleepless night, you go off the base, away from your military encampment, and shoot some civilians in the nearby town to relieve your frustrations. *Would you and your fellow soldiers regard your behaviour as understandable, forgivable, excusable?*

You are engaged in a coalition military operation in a foreign country where terrorists are active. You decide to 'teach them a lesson' by going into a nearby village and killing all the children in their schoolhouse. *Would you and your fellow soldiers regard your behaviour as understandable, forgivable, excusable?*

During a fierce firefight, enemy snipers manage to pick off and kill several of your fellow soldiers, including your most popular senior enlisted leader. The very next day, your commanding officer encourages all of you to go into a nearby village (populated by civilians who are probably sympathetic to the enemy) to kill the inhabitants and burn their village. *Would you and your fellow soldiers later regard the order and your subsequent behaviour as understandable, forgivable, excusable?*

Follow-up:

Instructor: 'Can we define some of the other principal features of this code that we impose on ourselves and agree to abide by as ethical leaders and military professionals?' [Write down suggestions on a whiteboard, piece of paper, or some other medium. Here are some examples the participants might suggest, or you can interject them if the discussion lags]:

The sacred trust of protecting non-combatants (e.g. young children or the elderly) caught between *both sides* of the conflict.

What about the well-being, the 'soul' of the warrior himself? Does following the Code provide protection for the warrior? Note that post-traumatic stress disorder (PTSD) is frequently linked to the guilt and regret experienced by combatants who have violated or witnessed violations of this code. [This is increasingly called 'moral injury'.]

Task 2. Discuss the situations.

Case study: Peacekeeping operation involving child combatants

A peacekeeping platoon was deployed as part of an international assistance effort to support a government facing armed insurgency. The unit was tasked with providing security and repelling a loosely organized rebel group advancing towards a major population centre. During the operation, the platoon came under fire, returned fire, and ultimately succeeded in pushing the insurgents back from the outskirts of the city.

When the unit returned, it became clear that the engagement had resulted in an unexpectedly high number of casualties within the peacekeeping force. Commanders couldn't understand how such a highly trained and well-equipped contingent had suffered significant losses against what was believed to be an undisciplined and lightly armed adversary. It was later discovered that many members of the opposing force were children, some of whom demonstrated combat skills, while others were visibly frightened and distressed. According to reports, several peacekeepers hesitated to engage child combatants, noting, 'This isn't what we came here to do – we didn't come here to shoot children.'

Discussion questions:

- Were the peacekeepers justified in their reluctance to fire upon child combatants? What alternative actions might they have taken under such conditions?
- What ethical concerns arise from the recruitment or forced involvement of children in armed conflict?
- Did the peacekeeping contingent uphold professional and ethical military standards by refraining from killing child combatants?

3.8. Emerging technologies and cybersecurity in the defence sector

The unleashed power of the atom has changed everything save our modes of thinking, and we thus drift toward unparalleled catastrophe.

– Albert Einstein, 1946

Ethical reflection on new military technologies must not be postponed until after their deployment. By then, the damage is already done.

– George R. Lucas Jr., 2016

Module objectives

To understand how emerging technologies and cybersecurity shape ethical decision-making in defence contexts, to identify the associated risks and dilemmas, and to critically assess institutional responses and accountability frameworks. Guided by IHL, international human rights law, just war theory, and military codes of conduct, participants will examine how specific technological capabilities – such as artificial intelligence (AI) for reconnaissance, target identification, and engagement; dual-use digital tools; and cyber capabilities – interact with core ethical principles, including distinction, proportionality, necessity, and responsibility. The training distinguishes between technological functions and their ethical or legal implications, covering issues such as surveillance and privacy, data governance, algorithmic bias, and challenges to meaningful human control. By the end of the session, participants will be equipped to promote responsible, lawful, and ethically grounded innovation in digital defence environments.

Key information

a. Emerging technologies – including AI, autonomous systems, biometric tools, and cybersecurity capabilities – are rapidly transforming defence operations, strategic planning, and decision-making structures.

b. While emerging technologies enhance military capabilities, they also introduce distinct ethical and legal risks (e.g. opaque algorithms, reduced human oversight, or increased surveillance), raising challenges related to accountability, transparency, bias, and the protection of civilians.

c. Cyber operations challenge traditional understanding of armed conflict and attribution, often falling within areas of contested applicability under international law, particularly when they affect civilian infrastructure or intrude on privacy rights.

d. The use of autonomous and AI-enabled systems in reconnaissance, target identification, and engagement raises questions about maintaining meaningful human control and oversight, ensuring proportionality and compliance with the principles of IHL.

e. Dual-use technologies complicate the boundaries between civilian and military domains, creating risks of misuse, overreach, or erosion of public trust – especially where regulation and oversight are insufficient.

f. Addressing dilemmas relating to emerging technologies requires robust institutional safeguards; ethical and legal review mechanisms that account for existing IHL obligations; and professional integrity in procurement, development, and deployment; to ensure that innovation remains consistent with ethical doctrine, legal standards, and democratic values.

Module content

Definition and forms of manifestation

Emerging technologies refer to a set of new and rapidly evolving tools that are transforming the way militaries operate in both combat and non-combat environments. These technologies include AI, decision-support systems (DSS), autonomous weapons, cyber capabilities, surveillance tools, space-based systems, and biotechnology. While these technologies offer specific operational advantages, they also introduce complex ethical and legal challenges – particularly in relation to human control, accountability, and compliance with IHL.

These systems are often dual-use, meaning they can serve both civilian and military functions. Their deployment, however, frequently occurs faster than the development of regulatory frameworks by which to govern them. Moreover, their ethical implications depend not just on how they are designed, but on how they are used, and by whom.

Example

Pegasus, developed by the Israeli company NSO Group, illustrates the dual-use risks and accountability challenges associated with advanced surveillance technologies. Although marketed as a counterterrorism capability, Pegasus enables remote and covert access to a target's smartphone – including the messages, microphone, camera, and location data – and its deployment has extended well beyond these stated purposes. Of the government bodies to whom the software has been sold, 51% are intelligence agencies, 38% law enforcement bodies, and 11% military institutions, indicating how such tools circulate across multiple security sectors with differing oversight mechanisms.[52]

These characteristics have enabled a range of uses in military and security contexts that raise ethical and governance concerns. During the 2020 Nagorno-Karabakh war, Azerbaijani authorities reportedly incorporated Pegasus into their wider military efforts by surveilling Armenian officials, journalists, and civil society members.[53] In the United Arab Emirates, the spyware has been linked to the monitoring of political rivals and critics under the umbrella of national security, with some reports suggesting its use alongside military

52 Stephanie Kirchgaessner, Paul Lewis, David Pegg, et al. 'Revealed: Leak uncovers global abuse of cyber-surveillance weapon', World News, *The Guardian* (18 July 2021), https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

53 Amnesty International, 'Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict' (25 May 2023), https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict

and intelligence activities in Yemen.[54] In Mexico, the military deployed Pegasus to surveil journalists investigating corruption and human rights abuses, despite official assurances that its use was limited to counterterrorism.[55] Collectively, these cases demonstrate how a dual-use surveillance tool can, in the absence of strong safeguards and oversight, be applied in ways that expand state surveillance capacities, blur boundaries between military and civilian targets, and weaken mechanisms of accountability and transparency.

Table 3 provides an overview of the most relevant emerging technologies for defence ethics, including brief definitions, their military use and operational advantages, and the ethical concerns they raise.

Table 3. An overview of emerging technologies

Definition	Military use and operational advantage	Key risks and ethical concerns
Artificial Intelligence		
AI: Systems that simulate human reasoning or learning. DSS: Tools that provide data-based advice to support decision-making.	Used for targeting, logistics, threat prediction, and real-time battlefield analysis.	Bias, hallucinations[56], lack of transparency, overreliance, erosion of human accountability.
Autonomous Weapons Systems		
Weapons that can select and engage targets without direct human input or real-time control.	Enables rapid response, force multiplication, reduced soldier exposure in high-risk environments.	Delegation of lethal decisions, unpredictability, accountability gaps.
Cyber operations and weapons		
Offensive or defensive operations conducted through digital networks to disrupt, manipulate, or disable.	Used for disabling infrastructure, espionage, psychological operations, and non-kinetic attacks.	Attribution difficulty, spillover to civilian systems, lack of legal clarity.
Surveillance biometrics and data analytics		
Technologies for collecting and analysing physical or behavioural data for identification or prediction.	Enhances intelligence, monitoring, and targeting capacities; supports perimeter and population control.	Privacy invasion, discriminatory profiling, misuse of civilian or sensitive data.
Remote and robotic systems		
Unmanned ground, aerial, or maritime systems used to perform military tasks with minimal human risk.	Logistics, reconnaissance, perimeter defence, explosive ordnance disposal, ISR missions.	Disconnection from ethical decision-making (reduced human involvement in use-of-force decisions, operators removed from on-scene context and cues), malfunction, dual-use ambiguity.

54 Anadolu Agency, 'UAE under fire for spying officials, activists in Yemen', Accessed 30 July 2025, https://www.aa.com.tr/en/middle-east/uae-under-fire-for-spying-officials-activists-in-yemen/2324007

55 Freedom House, 'Mexico: Freedom on the net 2023, country report', Accessed 30 July 2025, https://freedomhouse.org/country/mexico/freedom-net/2023

56 An AI hallucination occurs when an AI system generates information that appears plausible and credible, but is factually incorrect or entirely fabricated resulting from the model's reliance on probabilistic text generation rather than the validation of facts.

Space-based capabilities		
Satellites and orbital assets used for surveillance, communication, targeting, or early warning.	Global coverage, secure communication, GPS-guided weapons, strategic intelligence gathering.	Civilian dependency, weaponization of space, and infrastructure vulnerability.
Human enhancement and biotechnology		
Use of biological or technological interventions to enhance physical or cognitive military performance.	Increased endurance, resilience, mental acuity, or injury recovery among personnel.	Consent, inequality, health risks, and militarization of human body.
Quantum technologies		
Technologies leveraging quantum physics for computing, encryption, or sensing.	Future capabilities for secure communication, radar evasion, advanced surveillance.	Strategic instability, disruption of existing security systems, asymmetric tech race.
3D printing and additive manufacturing		
Layer-by-layer fabrication of weapons, equipment, or spare parts from digital files (3D models), enabling on-demand, on-site production of plastic or metal parts without traditional tooling.	On-site production of critical parts, rapid prototyping, logistical autonomy in remote settings.	Arms proliferation, lack of regulatory oversight, difficulty tracking distributed production.

When emerging technologies are used without ethical safeguards, the consequences can be severe. Soldiers and commanders may be held responsible for actions based on flawed or biased systems they do not fully control, and civilians may be wrongfully targeted or subjected to surveillance and profiling. Defence institutions risk eroding public trust, compromising operational integrity, and facing legal or political backlash. Even highly capable systems – if poorly understood or unchecked – can lead to unintended escalation, loss of life, or violations of international law.

Example

From the late 2000s onward, extensive remote-strike operations were conducted as part of a broader counterterrorism campaign aimed at eliminating high-value targets. These operations often relied on metadata analysis, pattern-of-life assessments, and other forms of remote sensing – methods that carried a significant risk of error. In one widely documented case, a strike on a civilian convoy resulted in at least a dozen deaths, most of them non-combatants. Independent human rights organizations and subsequent investigations later confirmed that the attack stemmed from flawed intelligence, making it one of several incidents in which remote targeting contributed to unlawful loss of civilian life.

A report to the international human rights community subsequently noted that these operations had caused civilian casualties and may have breached international humanitarian and human rights laws, emphasizing the need for greater transparency, accountability, and adherence to legal safeguards. Such incidents have damaged trust in counterterrorism efforts, reduced local cooperation, and raised profound ethical and legal questions about the deployment of remote-strike technologies without robust oversight mechanisms.

Emerging military technologies are advancing faster than the laws designed to regulate them. While IHL applies regardless of the technology used, it was developed in an era of conventional weapons. Key principles such as distinction, proportionality, precaution, and the obligation to conduct legal reviews of new weapons (Article 36 of Additional Protocol I) still offer critical guidance – but interpreting and applying these principles to AI-driven systems, cyber tools, or autonomous platforms raises increasingly complex questions. These technologies are often opaque, unpredictable, and deployed in dual-use environments, creating interpretive uncertainty rather than gaps in the law itself, and challenging how traditional legal assessments should be carried out in practice.

Beyond IHL, relevant norms exist across international human rights law, arms control treaties, data protection frameworks, and national procurement regulations, but none provide comprehensive or specific governance for these technologies. Many tools – such as cyber weapons or decision support systems – operate in areas where no treaty-based regulation exists and where there is limited or no consensus under customary international law. Ongoing discussions in UN forums, including the Group of Governmental Experts (GGE) on lethal autonomous weapons and Open-Ended Working Group on Information and Communication Technology (ICT), have made limited progress. As a result, regulatory oversight varies significantly between states, and ethical responsibility often falls to individual commanders and institutions operating without clear legal boundaries.

While states differ significantly in their access to emerging technologies – some developing domestic capabilities, others depending on foreign suppliers or private companies – this variation does not alter the underlying ethical obligations. Differences in technological sophistication shape how states employ these tools, but they do not change the requirement to uphold international norms. Ethical decision-making, accountability, and responsible conduct remain essential regardless of a state's capability level or degree of technological advancement. With this in mind, the following section examines a set of recurring ethical dilemmas that defence personnel may encounter when emerging technologies are deployed in practice, recognizing that ethical responsibility attaches to conduct, not to technological capacity.

Can we delegate decision-making to systems we do not fully understand?

Emerging technologies increasingly shape how military decisions are made – sometimes supporting human judgement and sometimes replacing it altogether. Autonomous weapons systems, AI-driven targeting tools, and cyber operations often function with limited transparency and limited human input. These systems promise speed, precision, and operational efficiency, but they also carry serious ethical risks, particularly when commanders do not fully understand how decisions are reached or what effects will follow.

One of the most pressing concerns is the loss of meaningful human control. When systems autonomously identify and engage targets, or when decision-support tools generate complex recommendations that users cannot verify, the nature of responsibility becomes unclear. Who is accountable when an AI-based system approves a strike that kills civilians? How much weight should a commander place on a machine-generated assessment they cannot explain?

Example: The black box problem

What is the 'black box problem'?

The black box problem refers to the lack of transparency in how complex technologies – particularly advanced AI systems – reach their conclusions. In many cases, this opacity stems not only from the fact that access to algorithms is restricted but also from the inherent technical complexity of machine-learning models, which can make their internal reasoning difficult to interpret, even for experts. When users cannot see or fully understand how a system processes information, they are left to either blindly trust or question its outputs. This creates significant ethical and operational challenges, especially in military contexts where the quality of decision-making and accountability have direct consequences for human lives.

Example: AI targeting in conflict

During the conflict, the Defence Forces reportedly used several AI-assisted systems, including The Gospel and Lavender, to accelerate targeting decisions. The Gospel was used to generate recommendations for strikes on infrastructure at high volume and speed, often beyond the capacity of human analysts to meaningfully review. Lavender identified individual targets – allegedly based on metadata – with operators sometimes spending as little as 20 seconds per approval.[57] One user described their role as having 'zero added-value as a human, apart from being a stamp of approval'.[58] These cases illustrate the black box problem: when decision-makers do not understand how systems reach their conclusions, and when human involvement is reduced to a procedural formality, meaningful human control is eroded and accountability becomes dangerously unclear.

These questions are further compounded by concerns about reliability and bias. Technically, AI systems are only as good as the data on which they are trained, meaning they can reproduce or amplify existing social, cultural, or operational biases. They may also exhibit specific failure modes – such as hallucinating plausible but false outputs, misidentifying individuals or objects, or failing to detect relevant behaviour – even when operating as intended. These technical shortcomings translate into ethical concerns when system outputs inform real-world decisions. Errors that lead to unjustified targeting, discriminatory outcomes, or unwarranted surveillance cannot be dismissed as mere technical glitches; they become ethical failures with concrete human consequences.

From the perspective of targeting, these risks are heightened. Technologies that rely on pattern recognition and probabilistic inference can blur the line between suspicion and threat, with metadata or past behaviour used to infer hostile intent. Such inferences may be acted upon even when the system lacks situational context or nuance. This raises serious issues under IHL, particularly regarding the principles of distinction (correctly identifying combatants versus civilians), proportionality (ensuring that expected civilian harm is not excessive), and precaution (verifying targets and minimizing risks to civilians). These challenges are especially acute in environments where civilian and military actors use overlapping technologies or infrastructure, such as phones, vehicles, or digital networks.

57 Michael N. Schmitt, 'Israel – Hamas 2024 Symposium – The Gospel, Lavender, and the Law of Armed Conflict', *Lieber Institute West Point* (28 June 2024), https://lieber.westpoint.edu/gospel-lavender-law-armed-conflict; Yuval Abraham, '"Lavender": The AI machine directing Israel's bombing spree in Gaza', *+972 Magazine* (3 April 2024), https://www.972mag.com/lavender-ai-israeli-army-gaza

58 Bethan McKernan and Harry Davies, '"The machine did it coldly": Israel used AI to identify 37,000 Hamas targets', World News, *The Guardian* (3 April 2024), https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes

Example

The U.S. Department of Defense launched Project Maven in 2017 to accelerate the integration of AI into military operations. The project aims to automate the analysis of a vast amount of surveillance footage, to detect, classify and track objects of interest such as vehicles or individuals. However, humans at the 18th Airborne Corps can correctly identify a tank 84% of the time, compared with Maven at around 60%. And experts say that number goes down to 30% on a snowy day.[59]

Cyber operations pose a related challenge. While not always automated, they can have unpredictable effects, including cascading failures across civilian systems such as hospitals, power grids, or communications. Because malware behaves dynamically and may spread across borders or systems, the full consequences of a cyberattack are often unknowable in advance – making ethical assessment difficult and complicating compliance with legal principles such as precaution and proportionality.

Example

The 2017 NotPetya cyberattack – initially targeting Ukrainian institutions – turned into a global incident. The cyber operation is believed to have been launched by Russian state actors under the guise of ransomware, while in fact NotPetya was a wiper malware designed to destroy data rather than extort payment. Though its intended target appeared to be Ukraine's financial, governmental and energy infrastructure, the malware spread uncontrollably across borders via widely used accounting software, affecting multinational companies such as Maersk, Merck, FedEx, and even hospital systems in the US and UK. The attack caused over $10 billion in damages globally and disrupted operations in sectors far removed from any conflict zone.

Together, these developments raise a common dilemma: How can ethical standards be upheld when humans are no longer the sole – or even primary – agents of decision-making? Emerging technologies offer powerful capabilities, but they also risk distancing moral responsibility from the actions taken in their name. This does not eliminate accountability, but it does demand new forms of scrutiny, transparency, and professional judgement in military operations. To meet these challenges, institutions must invest in robust safeguards and auditability mechanisms, clear human–machine teaming protocols that preserve meaningful human control, and, where necessary, legal and policy reforms that clarify responsibilities and ensure compliance with international norms.

Do surveillance and data collection undermine the values and objectives they aim to protect?

Surveillance technologies and data analytics systems are increasingly embedded in defence operations. These tools range from targeted intelligence-gathering technologies – such as facial recognition at checkpoints or biometric verification for access control – to broader data collection and monitoring systems, including wide-area biometric databases, social media analysis tools, and population-level pattern-detection platforms. While these capabilities are often used to enhance security, support threat identification, and inform operational decision-making, their ethical risks remain significant. The use of indiscriminate or large-scale data collection, particularly in conflict zones or occupied territories, raises concerns about privacy violations, the potential for chilling effects, and the risk of arbitrary or unjustified targeting.

59 Saleha Mohsin, 'Inside Project Maven, the US military's AI project', *Bloomberg.Com* (29 February 2024), https://www.bloomberg.com/news/newsletters/2024-02-29/inside-project-maven-the-us-military-s-ai-project

Individuals may be flagged on the basis of behavioural patterns or inferred associations that are poorly understood or misinterpreted by automated systems. In many cases, those subject to surveillance have no awareness of its use, no means to contest errors or challenge inclusion in databases, and no access to meaningful legal remedies.

Ethical concerns arise for different reasons, depending on how surveillance is implemented:

- **Scale:** Broad, population-level monitoring carries different risks than targeted intelligence gathering, particularly regarding privacy and proportionality
- **Transparency:** When individuals lack awareness of surveillance or its purpose, safeguards for contesting errors or abuse are weakened
- **Discriminatory application:** Uneven or biased deployment can disproportionately affect certain groups and undermine equality and fairness
- **Oversight and accountability:** Weak regulatory or institutional oversight increases the likelihood of misuse and reduces available avenues for redress.

These practices raise important human rights considerations and may undermine public confidence in defence institutions by blurring the line between legitimate security activities and broader population monitoring. Even when technically lawful, certain forms of surveillance may still be ethically problematic – particularly when they reinforce discriminatory patterns, disproportionately affect specific groups, or are applied unevenly across different segments of the population.

Example

Palantir Technologies has provided data integration and analytics tools to military, intelligence, and law enforcement agencies. Its platforms aggregate and analyse vast datasets – from biometric and facial recognition systems to social media activity and sensor inputs – to support threat identification and population monitoring. While marketed as tools for enhancing operational insight, Palantir's technologies have drawn significant criticism in both domestic and conflict settings. Across these contexts, human rights organizations have raised concerns about the company's failure to exercise due diligence in preventing rights abuse, warning that such tools risk enabling arbitrary targeting, reinforcing repression, and eroding public trust in defence institutions.

Do emerging technologies increase risk of civilian harm by blurring the lines between civilian and military space?

Emerging technologies such as cyber capabilities, AI-enabled decision support systems, satellite and geolocation services, commercial cloud platforms, and networked logistics systems increasingly operate across both civilian and military domains. These dual-use systems are frequently built on infrastructure that serves civilian populations while also supporting military communications, planning, and operational decision-making. As a result, the boundary between civilian and military objects becomes more difficult to interpret in practice.

This dual-use environment creates legal and ethical ambiguity, particularly regarding the IHL principle of distinction. Civilian infrastructure – such as data centres, telecommunications networks, commercial satellites, and cloud services – is now routinely used for military purposes. This means that actions aimed at legitimate military objectives may unintentionally affect protected civilian systems. For example, a cyber operation directed at a military application hosted on a civilian cloud platform could disrupt hospitals, schools, or financial

services. Similarly, surveillance drones operating in mixed civilian airspace may capture data on individuals with no connection to military activities, complicating assessments of necessity and proportionality.

These dynamics increase the risk of indiscriminate or disproportionate effects, especially in highly interconnected digital environments where civilian and military functions are technically intertwined. In such contexts, the ethical responsibility of commanders extends beyond identifying an intended military target: it requires anticipating the potential spillover effects on civilian populations and infrastructure, assessing whether dual-use systems can be lawfully targeted, and ensuring compliance with IHL despite the complexity introduced by emerging technologies.

Example

In 2025, Russian authorities began implementing daily mobile internet blackouts across much of the country so as to interfere with Ukrainian drones using civilian data networks for navigation. These shutdowns disrupted banking, transport, healthcare, and emergency services, impacting millions without warning. While intended as a defensive measure, the operation illustrates how emerging technologies that rely on shared infrastructure can produce disproportionate civilian harm – challenging the IHL principle of distinction and underscoring the ethical risks of blurred civilian–military boundaries.[60]

These developments illustrate that emerging technologies require not only improved anticipation of spillover effects, but also a broader reconsideration of existing ethical and legal frameworks. As civilian and military systems become increasingly entangled, structural measures are necessary to preserve civilian protections and ensure that operational decisions remain aligned with established principles of IHL.

To what extent can we rely on private companies in the defence sector?

Defence institutions increasingly depend on private companies to not only supply tools but also operate and manage the digital infrastructure on which modern military activities rely. This includes proprietary software, cloud services, surveillance platforms, satellite networks, and the algorithms that support AI-enabled decision-making. It is important to distinguish between operational reliance – using commercial tools in day-to-day activity – and strategic dependency, in which core defence functions cannot be performed without a private actor's cooperation or continued service. The latter creates more significant ethical and policy risks, as states may lack full control over systems critical to military effectiveness or civilian protection.

This dependency raises specific ethical concerns. Private companies are commercial actors; they are not bound by the same legal obligations, including IHL or military ethical frameworks. Yet their decisions – whether to restrict, update, modify, or terminate access to a system – may have direct implications for operational outcomes, the safety of personnel, and the protection of civilians. In extreme cases, commercial actors may effectively make decisions that shape the use of force, despite not being accountable under state-based command structures.

60 Nataliya Vasilyeva and Alina Lobzina, 'Russia counters Ukrainian drones by turning off Russians' mobile internet', World. *The New York Times* (28 July 2025), https://www.nytimes.com/2025/07/28/world/europe/russia-internet-blackouts-drones.html

Example

Elon Musk [@elonmusk]. (2025, March 9). Post on Starlink [Post]. X. https://x.com/elonmusk/status/1898612062533956047.

Since Russia's 2022 invasion, Ukraine has relied heavily on the Starlink satellite internet service provided by SpaceX for secure communications and drone coordination. In 2023, Elon Musk acknowledged restricting Starlink's use to prevent Ukrainian attacks on Russian-occupied territory, asserting that the system 'was not meant to be involved in wars'. This episode illustrates not only the influence a private actor can exert over military activity, but also the structural vulnerability created when essential military infrastructure is governed by private terms of service rather than binding agreements, oversight mechanisms, or contingency planning.[61]

These dynamics also complicate accountability and command responsibility. When a system fails, data is breached, or an AI tool produces harmful outputs, determining responsibility becomes difficult: was the cause a design flaw, user decision, contractual restriction, or corporate policy? Such ambiguity risks blurring lines between public and private actors and may hinder the enforcement of legal norms, including those governing command responsibility under IHL.

As militaries increasingly collaborate with start-ups – whose internal processes, transparency standards, and operational experience may vary widely – the need for safeguards becomes more pressing.[62] Ensuring that private-sector involvement does not compromise legal compliance, operational integrity, or the protection of civilians requires robust contractual controls, clear oversight mechanisms, rigorous due-diligence processes, ethical procurement standards, and technical audits. These measures help ensure that while private companies play a role in defence ecosystems, they do not exercise de facto control over decisions that carry legal and ethical significance for states.

When is efficiency unethical?

AI-enabled targeting promises faster and more accurate strikes with reduced risk to civilians, so, in theory, this aligns with IHL by increasing precision and limiting collateral damage. The central ethical dilemma, however, lies in the conflict between tactical efficiency and the strategic and moral responsibility that armed forces must uphold. Systems designed to accelerate target generation can, in practice, encourage rapid escalation and industrial-scale targeting that reduces opportunities for the deliberate human judgement required by the principles of distinction, proportionality, and precaution. Recent reporting on AI systems capable of producing thousands of strike targets in compressed timeframes raises a difficult question: when speed and volume become the defining metrics of success, does the space for ethical evaluation diminish? Even if each strike is individually lawful, there may be a point at which the pace and scale of lethal action challenge the moral foundations of military necessity.

61 PBS News, 'Elon Musk's refusal to provide Starlink support for Ukraine attack in Crimea raises questions for Pentagon' (11 September 2023), https://www.pbs.org/newshour/economy/elon-musks-refusal-to-provide-starlink-support-for-ukraine-attack-in-crimea-raises-questions-for-pentagon

62 Matthias Gebauer, Martin Hesse, Marcel Rosenbach, and Gerald Traufetter, 'Battlefield disruption: German military seeks to adapt as AI changes warfare', International. *Der Spiegel* (21 February 2025), https://www.spiegel.de/international/germany/battlefield-disruption-german-military-seeks-to-adapt-as-ai-changes-warfare-a-ebb36190-8b79-4e85-bd21-e765a9fc9857

Example

In one recent conflict, senior military leadership reported that once an automated targeting system was activated, it produced an unprecedented volume of targets each day – vastly exceeding the rate achievable through traditional intelligence methods. Subsequent conflicts have shown similar patterns, with the number of strikes conducted in short periods far surpassing those in earlier engagements of longer duration. These developments raise difficult ethical questions. When operational efficiency becomes the primary metric of success, does meaningful moral evaluation risk being overshadowed? Even if individual strikes satisfy legal requirements, is there a threshold at which the sheer pace and scale of lethal action challenge the underlying principles of military necessity, proportionality, and humane conduct?

Precision should not be confused with prudence. Ethical restraint in warfare is not only about legality; it is also about deliberation, proportionality, and humanity. Systems that accelerate action without ensuring space for human judgement risk undermining the very values they claim to uphold.

Good practice or solution? How can we ethically review emerging technologies?

Emerging technologies often evolve faster than the systems designed to govern them. Legal reviews, such as those required by Article 36 of Additional Protocol I to the Geneva Conventions, are intended to ensure that new weapons, means, or methods of warfare comply with international law. But when it comes to tools such as AI algorithms, cyber capabilities, or autonomous systems, standard review procedures may fall short.

Some technologies are developed incrementally or adapted from civilian applications, making it difficult to define when a ‘new weapon’ has been introduced. Others may appear legally compliant in isolation but pose ethical problems once integrated into complex systems or deployed at scale. For example, an AI system might support lawful targeting decisions under test conditions but produce unanticipated patterns or effects in live operations.

Ethical review must therefore go beyond checking formal legality. It should include questions of reliability, bias, accountability, civilian impact, and loss of human oversight. And it should apply not only at the deployment stage, but also during design, acquisition, and integration. This requires multidisciplinary input – legal, technical, operational, and ethical – supported by transparent procedures and institutional responsibility. The following box, titled ‘Legal and ethical review of emerging technologies’, illustrates steps that some states and actors have taken to this end:

Example: Legal and ethical review of emerging technologies

United States

The U.S. Department of Defense (DoD) was the first military in the world to publish AI ethics principles. This process began in 2018 when DoD released its AI Strategy, which identified as one of its pillars 'leading in military ethics and AI safety' and pledged to articulate its vision and guiding principles for using AI in a lawful and ethical manner. The following year, the Defense Innovation Board proposed developing AI ethics principles for the design, development, deployment, and use of AI for both combat and non-combat purposes. This led to the adoption of DoD's Ethical Principles for AI in 2020 that guide the development of military AI systems[63]:

DOD AI ETHICAL PRINCIPLES

These principles apply to all DoD AI capabilities, encompassing both combat and non-combat applications.

RESPONSIBLE: DoD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.

EQUITABLE: The Department will take deliberate steps to minimize unintended bias in AI capabilities.

TRACEABLE: The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedures and documentation.

RELIABLE: The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.

GOVERNABLE: The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

Source: DoD Memorandum, "Artificial Intelligence Ethical Principles for the Department of Defense" (Feb 2020)

In 2021, the Deputy Secretary of Defense reaffirmed the AI Ethical Principles and directed the Joint Artificial Intelligence Center (JAIC) to coordinate actions to accelerate the adoption and implementation of responsible AI. In 2022, the DoD released the Responsible AI (RAI) Strategy and Implementation Pathway, which outlines in further detail the steps needed to this end. The strategy identified trust as the key objective, which can be achieved only through the application and development of the following:

63 U.S. Department of Defense, 'DOD adopts ethical principles for artificial intelligence' (24 February 2020). Accessed 6 August 2025, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence

- **Existing legal, ethical, and policy frameworks:** LOAC, just war theory, defence ethics rules, weapons review, legal requirements, moral imperatives, moral agency, and human judgement
- **DoD AI ethical principles**
- **RAI strategy and implementation:** RAI governance, warfighter trust, AI product and acquisitions lifecycle, requirements validation, responsible AI ecosystem and AI workforce.

Since 2022, as part of this strategy and the Department's broader efforts to govern the development and use of emerging defence technologies – especially AI and autonomy – the DoD has taken several concrete steps. It established the Chief Digital and AI Office (CDAO) as the lead authority for data, analytics, and AI. It updated DoD Directive 3000.09, 'Autonomy in Weapon Systems' (Jan 2023), to preserve appropriate human judgement and build in safety guardrails. And in 2024 it issued Generative-AI 'Guidelines & Guardrails', with a companion GenAI toolkit, to set out permissible uses, security and data requirements, documentation and testing expectations, and to keep humans in the loop. Together, these measures move the DoD from high-level principles to operational guardrails – clear roles, documented processes, and testing that keep accountable humans in control.

United Kingdom

The Ministry of Defence 'Ambitious, Safe, Responsible' policy paper (2022) outlines ethical principles for AI use in defence, focusing on principles of responsibility, human control, reliability, understandability, and bias mitigation.[64] The same year the Defence Artificial Intelligence Centre (DAIC) began its operation working to integrating AI into the military.[65] Since then the centre has taken several concrete steps to integrate and scale the safe and responsible use of AI in defence:

- **Developing tools to evaluate AI solutions:** DAIC's AI Model Arena provides a standardised, vendor-neutral environment for testing model performance, reliability, robustness, and security – supporting more rigorous ethical and legal review of emerging AI systems before they are deployed.[66]
- **Launching early-market engagement for data-labelling capabilities:** By improving access to high-quality, well-labelled datasets, DAIC aims to reduce bias, improve model reliability, and strengthen the evidentiary basis for assessing compliance with IHL principles such as distinction and proportionality.[67]
- **Providing enabling guidance for safe and responsible AI across defence:** Through implementation of JSP 936 and related guidance, DAIC is establishing formal processes – such as documentation standards and risk-management frameworks – that embed accountability, transparency, and auditable oversight into AI development and procurement.[68]

64 GOV.UK, 'Ambitious, safe, responsible: Our approach to the delivery of AI-enabled capability in defence' (15 June 2022). Accessed 5 August 2025, https://www.gov.uk/government/publications/ambitious-safe-responsible-our-approach-to-the-delivery-of-ai-enabled-capability-in-defence/ambitious-safe-responsible-our-approach-to-the-delivery-of-ai-enabled-capability-in-defence

65 GOV.UK, 'Defence Artificial Intelligence Centre', Accessed 5 August 2025, https://www.gov.uk/government/groups/defence-artificial-intelligence-centre

66 Ministry of Defence, 'Launching the AI Model Arena', GOV.UK News (10 November 2025), https://www.gov.uk/government/news/launching-the-ai-model-arena

67 Ministry of Defence, 'Early market engagement event for the delivery of artificial intelligence (AI) data labelling capabilities', Find a Tender Notice 2025/S 000-001229 (14 January 2025), https://www.find-tender.service.gov.uk/Notice/001229-2025?origin=SearchResults&p=1636

68 Ministry of Defence, 'JSP 936: Dependable artificial intelligence (AI) in defence – Part 1: Directive' (13 November 2024), https://www.gov.uk/government/publications/jsp-936-dependable-artificial-intelligence-ai-in-defence-part-1-directive

- **Championing common AI services and building a coherent defence AI ecosystem:** Drawing on the vision set out in the Defence AI Playbook, DAIC promotes shared platforms and model pipelines (such as those for imagery analysis or edge-AI testing) to enable consistent assurance procedures and ensure that emerging AI capabilities are evaluated within a controlled, ethically governed defence environment.[69]

France

In 2019, France's AI Task Force Report recommended creating a defence ethics committee to ensure that emerging technologies would be developed in line with IHL and ethical standards.[70] The Defence Ethics Committee (COMEDEF) was formally established on 10 January 2020, composed of 18 civilian and military experts drawn from fields such as law, engineering, medicine, philosophy, and the armed forces. Its mandate is to provide independent ethical opinions and recommendations on the evolution of the profession of arms and the integration of new technologies in defence.[71] Since its creation, COMEDEF has published a series of substantive viewpoints on emerging technologies that illustrate its role in shaping ethical boundaries for the French Armed Forces:

- **Viewpoint on the augmented soldier (2020):** The committee's first major viewpoint addressed the concept of the 'augmented soldier'. It acknowledged the operational benefits of physical, cognitive, or psychological enhancements but stressed that all augmentations must respect human dignity and IHL. Invasive modifications such as implants, drugs, or genetic interventions were considered particularly sensitive, with explicit prohibitions on any technology that might undermine free will, reduce controlled use of force, or amount to eugenics. The committee also insisted on reversibility, informed consent wherever possible, and medical oversight throughout the life cycle of augmentation, underlining the importance of long-term reintegration of soldiers into civilian life.
- **Viewpoint on the integration of autonomy into lethal weapon systems (2021):** In its 2021 opinion, the committee took a firm stance against fully autonomous lethal weapon systems (LAWS), judging them incompatible with IHL, military ethics, and the constitutional principle of human responsibility in the use of armed force. It allowed, however, for the development and use of partially autonomous lethal weapon systems (PALWS) under strict safeguards, providing human command and accountability were maintained. The viewpoint introduced a '5Cs' framework – command, control of risks, compliance, competence, and confidence – as the conditions for ensuring ethical and lawful use of autonomy in weapons, while warning against the misleading use of anthropomorphic terms such as 'autonomous' or 'intelligent' when referring to machines.
- **Viewpoint on the digital environment of combatants (2022):** In 2022, the committee examined the growing digitalisation of the battlefield. It welcomed the potential of digital tools to improve operational effectiveness but warned of new vulnerabilities such as cyberattacks, cognitive overload, and distorted situational awareness. It emphasized the continued primacy of human responsibility for all decisions supported by digital systems, calling for resilience training to prepare soldiers for degraded conditions, systematic legality checks on new tools, and awareness of risks posed by personal digital devices used in military contexts. The viewpoint underlined that ethical oversight must extend not only to technologies themselves but also to their psychological effects on combatants.

69 Ministry of Defence, *The Defence AI Playbook* (January 2024), https://assets.publishing.service.gov.uk/media/65bb75fa21f73f0014e0ba51/Defence_AI_Playbook.pdf

70 Report of the AI Task Force, *Artificial Intelligence in Support of Defence*, Ministry of the Armed Forces (September 2019).

71 The Defence Ethics Committee, *Ministry of the Armed Forces*, https://www.defense.gouv.fr/comite-dethique-defense

- **Viewpoint on the role of civil actors in a comprehensive defence strategy (2023):** The committee's 2023 viewpoint analysed the growing involvement of civilian actors in areas of conflict traditionally reserved for the military. It strongly rejected any 'privatization of war' or delegation of armed force to private companies, but recognized that civil society and private expertise could play a legitimate role in national defence under certain conditions. In particular, it highlighted the value of partnerships with open-source intelligence communities (OSINT) and cyber specialists to strengthen national resilience, while insisting that these contributions remain clearly bounded by law and ethical responsibility.
- **Viewpoint on the use of artificial intelligence technologies by the French Armed Forces (2025):** Most recently, the committee issued an extensive viewpoint on AI in defence. It reaffirmed that AI applications are subject to the same rules of IHL as any other military technology, and called for clear chains of accountability across the lifecycle of AI systems – from developers to operators and commanders. The viewpoint stressed the need for continuous testing, verification, and validation, and for maintaining human primacy in decision-making, with automation adjustable to operational context. It also underscored the importance of sovereign control over AI systems and training data, balanced with interoperability with allies, and encouraged studies on the long-term organizational and human effects of AI adoption in the armed forces.

NATO

NATO has adopted 'Principles of Responsible Use for AI in Defence' (2021), which include principles of lawfulness, responsibility and accountability, explainability and traceability, reliability, governability and bias mitigation. In 2024, NATO revised the AI Strategy, by updating the outcomes and adding new ones, which among others included[72]:

- A growing range of standards, assessment templates, review processes, and other tools and good practices to operationalise the responsible adoption of AI across the Alliance;
- A deeper understanding of AI by, and its implications for, the Alliance, informed by the results of the 360-degree monitoring of evolving AI and data technology trends. This understanding will include the opportunities and risks of AI, including its use by potential adversaries and strategic competitors;
- Key elements of an Alliance-wide AI Testing, Evaluation, Verification & Validation (TEV&V) landscape able to support the adoption of responsible AI. These elements will utilize the network of Defence Innovation Accelerator for the North Atlantic (DIANA) affiliated Test Centres;
- An increased contribution to shaping norms and standards for the responsible use of AI in defence and security. This contribution will be through the Alliance's engagement with NATO partners, international organizations, Allied industry and academia, as applicable; and
- Measures for addressing convergence between AI and other emerging disruptive technologies (EDTs).
- NATO needs to strengthen its understanding of the landscape and maturity of services, skilled testers, public and private AI safety bodies and accreditation and certification functions. Allies and NATO need to be able to access and use specialised laboratories, sandboxes and testing facilities. This will allow NATO to determine the opportunities and challenges, as well as to develop a baseline recommendation of best practices in TEV&V and certification of AI technologies.

72 NATO, 'Summary of NATO's revised artificial intelligence (AI) strategy' (10 July 2024). Accessed 5 August 2025, https://www.nato.int/cps/en/natohq/official_texts_227237.htm

In a landscape of accelerating technological change, rigorous and anticipatory review is one of the few safeguards available to ensure that emerging capabilities align with the values and obligations of lawful and ethical military conduct.

Remember that

- Emerging technology change military capabilities, not the ethical and legal obligations governing their use.
- Technological efficiency and autonomy do not replace human judgement or responsibility, and risk weakening accountability where meaningful human control is not preserved.
- AI – and data-driven tools can amplify bias, error and civilian harm when used without robust safeguards.
- Cyber operations and digital systems may produce indirect or cascading effects that challenge distinction, proportionality, and precaution.
- Dual-use technologies complicate civilian-military boundaries and require heightened care to prevent unintended harm.
- Ethical and legal review must extend across the full lifecycle of emerging technologies, from design and procurement to deployment and adaptation.

Check-your-skills exercises

Task 1. 'Black box – Operation Night Falcon'

Objectives:

- To simulate the challenges of decision-making with AI-assisted systems and fragmented intelligence.
- To illustrate how bias, uncertainty, and accountability gaps shape strike decisions.
- To promote reflection on thresholds of certainty and proportionality in military ethics.

Duration: 45–60 minutes

Group size: 12–25 participants (4 groups)

Materials needed:

- Printed role cards (or QR codes for digital access)
- Pens, flipcharts, or whiteboard

Instructions:

1. Introduction (5 minutes):

Instructor frames the scenario: 'You are part of a multinational task force deciding whether to launch a drone strike against a high-profile target. Each group will receive different information, reflecting how intelligence is fragmented across systems. The commanders will make the final decision. Remember: this is about ethical reasoning, not just tactical success.'

2. Role assignment and preparation (10 minutes):

- Divide participants into three groups of analysts (Raw Data, AI Output, Context) and one group of commanders.
- Distribute the role cards. Each analyst group must review their info and agree on one clear conclusion using a five-point certainty scale: *Very unlikely / Unlikely / Uncertain / Likely / Very likely.*
- Commanders, before hearing the groups of analysts, decide on their thresholds:
  - What minimum confidence in target presence justifies a strike?
  - What is the maximum acceptable risk of civilian harm?

Sample role cards:

Group 1: Data analysts

Your info:

- Drone feed: 3 adult males entered the building at 21:40.
- One matches the target's height and build (thermal imagery).
- Two carried large bags (contents unknown).
- Phone linked to the high-value target pinged twice in the last hour near this building.
- One man wore a long white robe (common civilian clothing).
- Children were seen outside earlier in the day, but no clear signs of children at night.

Hidden bias: Intelligence officers are under pressure after several recent failures to capture the target; they may be inclined to interpret ambiguous signs as confirmation.

Your task: Based on this information, how likely is it that the high-profile target is in the building? Choose one: *Very unlikely / Unlikely / Uncertain / Likely / Very likely*
Give *one* conclusion to the commanders.

Group 2: AI system output

Your info:

- AI system reports 92% probability target is inside.
- Facial recognition confidence: 85%, based on partial face from low-light camera.
- Movement pattern analysis consistent with target's past behaviour.
- Known issue: false positives in low-light conditions.
- Vendor's recent upgrade report says error rate has improved significantly (though not independently verified).

Hidden bias: System trained mainly on young male profiles from this region, making false matches with local men more likely. Developers are incentivized to present it as 'combat proven'.

Your task: Based on this information, how reliable is the AI system's assessment in this case?
Choose one: *Very unlikely / Unlikely / Uncertain / Likely / Very likely*
Give *one* conclusion to the commanders.

Group 3: Context and legal considerations

Your info:

- The building is in a residential neighbourhood.
- Thermal scan shows no obvious civilian activity at this hour.
- Local reports: families often leave the building in the evenings for communal gatherings.
- Civilian presence cannot be ruled out, but appears limited right now.
- Military lawyers remind you of IHL: distinction and proportionality.

Hidden bias: Local informants are paid by coalition forces; they tend to downplay civilian presence to encourage strikes. Reports of evening absences are anecdotal and unverified.

Your task: Based on this information, how likely is it that a strike would cause civilian harm?
Choose one: *Very unlikely / Unlikely / Uncertain / Likely / Very likely*
Give *one* conclusion to the commanders.

Group 4: Commanders

Preparation (before hearing others):

- Decide your thresholds:
  - What minimum confidence in target presence would justify a strike?
  - What is the maximum acceptable likelihood of civilian harm?
- Record these thresholds on your sheet.

Decision (after hearing others): Choose one.

- Strike now
- Do not strike
- Request more information

Justify your decision to the whole group.

3. Group work (10–15 minutes):

Each group discusses and agrees on its conclusion. They must be concise: one sentence for Commanders.

4. Reporting to the commanders (5–7 minutes):

- Each analyst group presents its one-line conclusion.
- Commanders record the input, then deliberate and announce their decision: Strike now / Do not strike / Request more information.
- Commanders must justify their decision to the plenary.

5. Debrief and discussion (15–20 minutes):

Facilitator guides reflection with questions such as:

- How confident did you feel in your group's conclusion?
- Did the AI system's probability overshadow human/contextual input?
- How did pre-set thresholds affect the commanders' final decision?
- What biases may have influenced your assessment? (confirmation bias, algorithmic bias, source bias)
- Who should be accountable if the strike kills civilians – analysts, developers, or commanders?
- How does this exercise mirror the *black box problem* in emerging technologies?

6. Expected outcomes:

- Participants experience the conflict of making life-and-death decisions with fragmented, biased, and uncertain information.
- Recognition of how AI probabilities can dominate, even when flawed.
- Awareness that biases (confirmation bias, algorithmic bias, informant bias) can skew conclusions and make strikes seem more justified than they are.
- Insight into the challenge of setting thresholds for action under uncertainty and proportionality constraints.
- Deeper appreciation of accountability dilemmas when technology mediates ethical decision-making.

04

Ethical decision-making in the defence sector

What happens when we carry these professional ideals into deployment or combat? Even worse, what is often likely to happen if we don't? Can we call upon ethics and good judgement at will, or (as Aristotle suggested), are these matters of lifelong habituation, for which 'practice makes perfect'? Wrestling in advance with relevant case studies that identify instances of unethical and unprofessional conduct can be helpful training. So can puzzling over genuine moral dilemmas (and tests of integrity) that may arise in the normal course of events, as well as in the stress of combat.

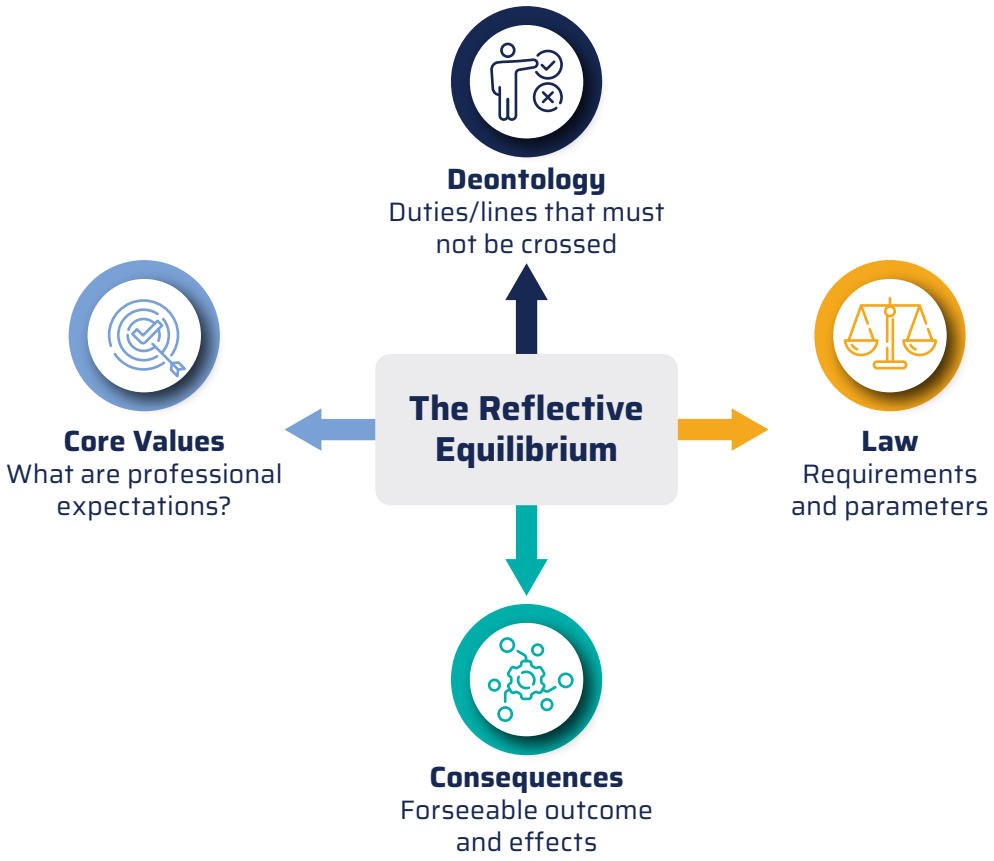

Figure 6. The ethical element of decision-making

One helpful way to accomplish this is through group discussion of case studies that invite us to apply some of the knowledge and procedures – such as the ethical decision-making model in Fig. 6 – that we have reviewed in these modules. Remember that the point of the model is to help us gather all relevant information about the crisis situation, consider what is the central problem or problems at stake, who the relevant 'stakeholders' (people facing difficult decisions, and others affected by them) are, and the likely outcomes of different choices and strategies that we might contemplate.

Figures 6 and 7 are designed to guide personnel through a clear, structured process when facing an ethical dilemma in the defence sector. This process is applicable in a variety of contexts, from routine administrative decisions and logistical planning to high-pressure operational scenarios in deployment or combat. The model ensures that decisions are not made solely on instinct or under immediate pressure, but instead are informed by a thorough and transparent consideration of facts, principles, and consequences.

Identify the problem

Clearly define the ethical dilemma in simple terms. Avoid getting lost in minor details; instead, focus on the main conflict of values or duties.

> *Ask: What exactly is the moral question here? For example, 'Should I report a fellow officer's misconduct even if it may harm unit cohesion?'*

This step frames the entire decision-making process, ensuring everyone is working from the same understanding of the issue.

Gather facts

- Collect all available information before acting. This includes operational intelligence, orders, applicable laws, and situational details.
- Avoid assumptions – distinguish between verified facts and rumours or incomplete information.

> *Example: Before deciding on an evacuation plan, confirm the number of civilians, security threats, and available resources.*

Identify stakeholders

Determine who will be directly or indirectly affected by the decision. Stakeholders often include:

- Fellow personnel and subordinates
- Civilians (local population, displaced persons)
- The chain of command and political leadership
- Partner forces, allies, and international organizations
- The broader public and media.

> *Example: Choosing a particular security checkpoint procedure may affect soldiers, local vendors, and aid workers differently.*

Consider obligations and duties

- Review legal frameworks: national laws, IHL, human rights law.
- Consult military codes of conduct, rules of engagement, and operational guidelines.
- Remember professional standards and personal moral commitments – not every obligation is written in law.

Example: You may be legally permitted to withhold certain information, but your duty to transparency and trust with partner forces may compel disclosure.

Examine possible consequences

- Assess the short – and long-term impact of each option on operational success, ethical integrity, and public perception.
- Consider both intended and unintended consequences, for example, how a tactical action today might influence civilian trust tomorrow.
- Use 'what if' scenarios to anticipate risks and benefits for each choice.

Test against core values

Ask whether the proposed action aligns with institutional and personal values such as:

- Integrity and honesty
- Fairness and impartiality
- Respect for human rights
- Mission effectiveness and safety of personnel.

Example: If a decision compromises fairness or endangers civilians, it likely fails the values test, even if it offers short-term tactical gains.

Decide and act

- Choose the option that best balances obligations, consequences, and values.
- Once the decision is made, communicate it clearly to all relevant actors.
- Ensure the action is implemented consistently with the reasoning process used to justify it.

Review the outcome

- After the action, evaluate the results: Did it resolve the problem? Were there unforeseen consequences?
- Document any lessons learned and integrate them into future decision-making and training.

Example: If an operational choice led to unintended civilian harm, assess how earlier steps in the process could have identified that risk.

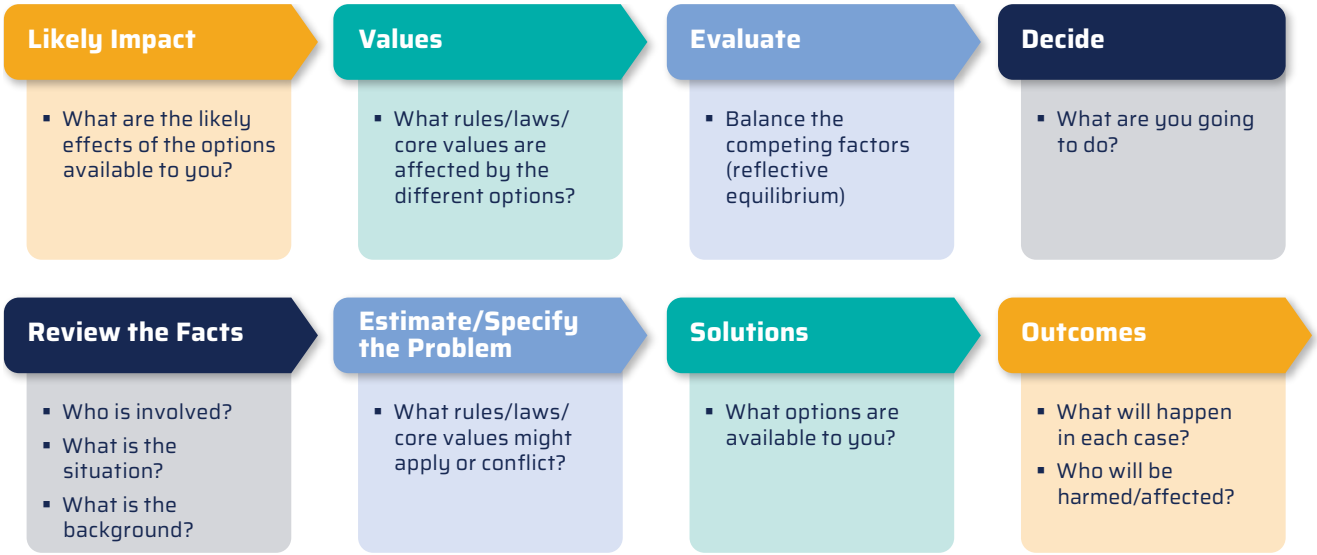

Figure 7. Ethical decision making

Let us remind ourselves that the goal of these deliberations is to consider and balance all the competing interests and moral decision-making criteria (duties and obligations, hoped-for good results, etc.) that we call 'reflective equilibrium', in which we call upon our best instincts and intuitions. Our goal is certainly to reach the best decision possible, but also to carefully consider how poor deliberation, bad judgement, or careless lack of due care and caution can bring about disastrous results for our unit, our personnel, the military itself, and society generally. With that in mind, let us once more review the decision-making model itself, and try it out on the cases that follow.

Ethical decision-making in military operations

A tragic incident during an international military deployment offers a powerful illustration of the complexities of ethical decision-making in the defence sector. During a combat operation, a group of soldiers opened fire with indirect and direct weapons toward positions believed to be held by hostile forces. Several munitions, however, struck a nearby village, resulting in the deaths of multiple civilians. The soldiers involved were subsequently charged with severe offences, including unlawful killing, and faced the prospect of long-term imprisonment.

The unit had been insufficiently prepared for the mission. Strategic decisions to expand the deployment had been made hastily, and the contingent suffered from inadequate equipment, training, and communications. Intelligence support that the soldiers expected was not provided until after the incident, when investigators began interrogations and controlling information flows. As a result, the soldiers became entangled in political narratives and were publicly portrayed as the sole culprits.

The legal proceedings extended over many years. The case led to what became known informally as a 'syndrome' among deployed personnel – a hesitation or paralysis in operational decision-making driven by fear of legal repercussions, which in turn discouraged proactive engagement in combat situations. This incident came to symbolize broader failures within both political and military structures, highlighting issues such as inadequate preparation, lack of equipment, poor coordination, and the political instrumentalization of front-line personnel. It exposed deep systemic problems and significantly affected the armed forces' internal culture, influencing perceptions of responsibility, loyalty, and accountability.

The events also revealed a clear distinction between ethical and unethical approaches to decision-making. Ethical decisions were evident in the behaviour of soldiers who, despite chaos and pressure, sought to protect civilian lives and carry out their duties in accordance with the rules of war. Their actions were motivated by a sense of responsibility, loyalty to their colleagues, and an awareness of the moral consequences of every shot. Even under enormous political pressure, they refused to admit to acts they had not committed, demonstrating moral courage and professionalism in difficult combat conditions.

Political and bureaucratic decision-making surrounding the deployment, however, reflected serious ethical shortcomings. Key policy choices were made without adequate preparation, exposing personnel to avoidable risks. Certain security services appeared to use the investigation to advance political narratives rather than to establish objective facts or ensure fairness. The manipulation of information, the pursuit of political advantage, and the absence of accountability among decision-makers exemplified unethical behaviour that disregarded individual welfare and fundamental moral principles.

Overall, this case underscores that ethical decision-making in military and political environments requires careful consideration of consequences, respect for human life, and adherence to moral norms. By contrast, decisions driven by political expediency or bureaucratic interests – without regard for safety, justice, or truth – can have devastating consequences for both individuals and the institution as a whole.

Check-your-skills exercises

Task 1. Interactive discussion-based exercises

These case studies are designed as interactive discussion-based exercises, are based on real-world incidents, and should be approached as learning opportunities, not just as historical reviews.

Objective: To help participants identify, analyse, and respond to ethical dilemmas in defence sector operations.

Instructions:

1. Introduce the case briefly without revealing the full details of the misconduct right away – let participants form their own judgements as the facts unfold.
2. Ask the discussion questions or share them in written form.
3. Ask participants to make ethical decisions.
4. Record participant responses on a flip chart.

Case study 1

Background:

A major procurement scandal arose when a senior civilian official responsible for defence acquisitions was found to have improperly influenced a multi-billion-dollar contract involving the long-term lease of military aircraft. The proposal involved leasing 100 replacement airframes over a decade – an arrangement significantly more expensive than purchasing them outright, according to internal auditors. Uniformed leadership objected that such a lease contradicted established acquisition policy, and the procurement process lacked the standard competitive review.

Despite these concerns, the deal moved forward under the direction of the senior official, who collaborated with an elected policymaker to circumvent normal procedures. Communications later revealed that the official had pushed for the lease arrangement while simultaneously securing future employment with the contractor offering the aircraft. The same contractor had previously hired a close family member of the official, reportedly with her assistance.

Operational urgency formed part of the backdrop: several older aircraft in service had suffered serious mechanical failures, including crashes resulting in fatalities. This created pressure to accelerate the acquisition of replacements, even though standard procurement protocols had not been met.

Key ethical and integrity issues:

- Improper influence and personal benefit in procurement decisions.
- Abuse of public office for personal or familial advantage.
- Conflict between urgent operational needs and compliance with acquisition rules.
- Erosion of public trust and the appearance of impropriety.

Discussion questions:

- Given the urgent requirement for replacement aircraft, does this situation represent a clear case of corruption or something more complex?
- If the official believed the lease solved a critical procurement challenge, could accepting special treatment from the contractor ever be justified?
- Does this scenario represent a genuine ethical dilemma or simply a failure of personal integrity?

Facilitator notes (debrief):

- Emphasize that operational urgency does not justify circumventing legal frameworks or accepting personal benefits.
- Clarify the difference between a true ethical dilemma – where legitimate values are in conflict – and an integrity violation.
- Link the case to broader principles of COI, accountability, and the importance of public trust in defence procurement.

Case study 2

Background:

During overseas deployments, naval vessels routinely stop at foreign ports for rest, resupply, and maintenance. Prior to these visits, ship crews often communicate their planned movements to approved service providers responsible for tasks such as waste removal, refuelling, restocking of food and supplies, and other port-based support activities. For security reasons, however, planned ship movements are highly sensitive and should not be disclosed outside authorized channels.

Over many years, the chief executive of a regional port-services company cultivated extensive corrupt relationships with numerous naval officers. These officers were provided with bribes – including cash, luxury travel, expensive gifts, entertainment, and other personal benefits – in exchange for releasing restricted information about the planned movements of ships and submarines.

According to later legal findings, the company used this information to manipulate port calls so that vessels would be directed to locations under its control. Once there, and with minimal oversight, the company systematically overcharged for services such as fuel, tugboats, barges, food, water, and waste removal. Senior officers were also encouraged to produce letters of commendation praising the company's performance, thereby strengthening its reputation and securing future business.

Key ethical and integrity issues:

- Unlawful disclosure of sensitive operational information.
- Long-term systemic corruption involving senior personnel.
- Fraudulent billing and misuse of public funds.
- Pressure placed on junior personnel to cooperate with corrupt practices.

Discussion questions:

- If you served as the ship's communications officer, would you follow an order directing you to release sensitive movement information to a contractor?
- If you were responsible for approving invoices, would you authorize inflated bills if senior officers expected you to?
- Are junior officers obligated to refuse such arrangements and report misconduct by senior personnel?

Facilitator notes (debrief):

- Emphasize that legal and ethical duties require the protection of sensitive information, even when contrary orders are given.
- Explore the conflict between loyalty to the chain of command and the duty to uphold law, integrity, and public trust.
- Discuss available protections and reporting channels for personnel who witness wrongdoing.
- Highlight how minor ethical compromises, if left unchecked, can evolve into pervasive systemic corruption.

Concluding remarks

This toolkit has been developed as a practical foundational resource to strengthen ethical decision-making, integrity, and professionalism in the defence and security sector. It is not intended to be exhaustive, nor does it prescribe a single model for ethical conduct. Rather, it seeks to provide military and civilian institutions with concrete guidance, tools, and learning methods to support the translation of ethical principles into everyday practice.

Recognizing that ethical challenges, organizational cultures, and operational realities differ across contexts, the toolkit is designed to be adaptable. It can be tailored to specific institutional needs, cultural environments, and operational settings. It uses examples, language, and training approaches that are most relevant to the users. The inclusion of case studies, practical exercises, and discussion prompts is intended to facilitate this contextualization and support engagement.

There remains much to be learned about how best to strengthen ethical culture and ethical leadership in complex and high-pressure defence environments. DCAF looks forward to continuing to support learning, dialogue, and exchange with partners, and to further developing and refining this toolkit as institutions share experiences and build collective knowledge in this critical area.

Further reading

Buckley, John, and George Kassimeris, eds., *Ashgate Research Companion to Modern Warfare* (London: Ashgate, 2010).

Carrick, Don, James Connelly, and Paul Robinson, eds., *Ethics Education for Irregular Warfare* (London: Ashgate, 2009).

Christopher, Paul, *The Ethics of War and Peace*. 2nd edn. (Upper Saddle River, NJ: Prentice-Hall, 1999).

Coady, C. A. J., *Morality and Political Violence* (Cambridge, UK: Cambridge University Press, 2008).

Coates, A. J., *The Ethics of War* (Manchester, UK: Manchester University Press, 1997).

Coleman, Stephen, *Military Ethics* (Oxford: Oxford University Press, 2012).

Cook, Martin L., *The Moral Warrior* (Albany: State University of New York Press, 2004).

French, Shannon E., *The Code of the Warrior* (Lanham, MD: Rowman and Littlefield, 2003). Revised 2nd edn. (2016).

The Geneva Conventions of 1949 and their Additional Protocols. https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols.

The Hague Conventions of 1899 and 1907. https://www.scribd.com/document/251305296/Hague-Conventions-of-1899-and-1907.

Hensel, Howard M., *The Prism of Just War: Asian and Western Perspectives on the Legitimate Use of Military Force* (London: Ashgate, 2010).

Ignatieff, Michael, *The Warrior's Honor: Ethnic War and the Modern Conscience* (New York: Henry Holt, 1998).

Kelsay, John, *Arguing the Just War in Islam* (Cambridge, MA: Harvard University Press, 2009).

Lucas, George R., Jr., ed., *The Routledge Handbook on Military Ethics* (London: Routledge, 2015).

Lucas, George, *Military Ethics: What Everyone Needs to Know* (New York: Oxford University Press, 2016).

Lucas, George, *Ethics and Cyberwarfare: The Quest for Responsible Security in the Age of Digital Warfare* (Oxford: Oxford University Press, 2017).

Lucas, George, *Ethics and Military Strategy in the 21st Century: Moving Beyond Clausewitz* (Oxford: Routledge, 2019).

Orend, Brian, *On War: A Dialogue* (Lanham, MD: Rowman & Littlefield, 2009).

Orend, Brian, *The Morality of War*. Rev. and exp. 2nd edn. (Peterborough, ON: Broadview, 2013).

Reichberg, Greg, and Henrik Syse, eds., *Religion, War and Ethics: A Sourcebook of Textual Traditions* (Cambridge, UK: Cambridge University Press, 2014).

Reichberg, Gregory S., Henrik L. Syse, and Endry Begby, eds., *The Ethics of War: Classical and Contemporary Readings* (Oxford: Blackwell, 2003).

Robinson, Paul, Nigel de Lee, and Don Carrick, eds., *Ethics Education in the Military* (London: Ashgate, 2008).

Roy, Kaushik, *Hinduism and the Ethics of Warfare in South Asia: From Antiquity to the Present* (Cambridge, UK: Cambridge University Press, 2012).

Scharre, Paul, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton &Co, 2018).

Schmitt, Michael N., ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, UK: Cambridge University Press, 2013).

Schmitt, Michael N., ed., *Tallinn Manual 2.0: International Law Applicable to Cyber Operations* (Cambridge, UK: Cambridge University Press, 2017).

Syse, Henrik, and Gregory Reichberg, eds., *Ethics, Nationalism, and Just War: Medieval and Contemporary Perspectives* (Washington, DC: Catholic University of America Press, 2007).

Tagarev, Todor, ed., *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva, Switzerland: Geneva Centre for the Democratic Control of Armed Forces, 2010).

Walzer, Michael, *Arguing about War* (New Haven, CT: Yale University Press, 2004).

Walzer, Michael, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 4th edn. (New York: Basic Books, 2006).

Yomamato, Tsunetomo, *Bushido: The Way of the Samuri*, translated by Minoru Tanaka (Garden City Park, NY: Square One, 2002).

Annex I

Temptations of command

Good people given the chance and authority to command may be tempted to abuse or misuse their authority. The top ten temptations, ranked by frequency, are:

1. **Falsifying, Massaging, or Manipulating Information or Data.** Participants identified that many senior leaders face a real temptation to be less than candid and honest, or even manipulative, when presenting information and data attached to their positions. This potential misuse of information/data has any number of causes, including paperwork exhaustion, time constraints, a desire to protect individuals/operations/organizations, and/or a self-serving willingness to personally benefit or make oneself look more successful. Participants noted this issue is a very pervasive temptation given the military's competitive, information-rich, and data-driven environment.

2. **Misuse of Government Funds/Resources/Personnel.** To enable them to complete the mission, leaders at all levels are entrusted with significant monetary and other tangible government resources that, without due diligence and attention, can be misused. Such mishandling might result in unauthorized pay reimbursements or improper personal use of government vehicles or other equipment. At the same time, the misuse of military personnel for personal benefit also surfaced as a real temptation. Employing these resources for personal advantage is a potential temptation that senior leaders must always address and avoid.

3. **Inappropriate Sexual Relationships.** The issue of inappropriate sexual relations quickly emerged in these discussions as a potential Achilles' heel for many senior leaders, despite the military's exceptionally strong prohibition against sexual harassment, assault, fraternization, and adultery. Participants highlighted many explanations for allowing this powerful temptation to grow into actual wrongful behavior, such as extended separations from loved ones, isolation and loneliness, stress-related sex, and hubris.

4. **Alcohol/Substance Abuse.** Any discussion of temptation in military circles will always include a discussion of alcohol, and our participants were no exception. They made the case that, although the military formally frowns on alcohol abuse, the military culture as a whole is still accepting and tolerant of alcohol consumption, which can create significant problems for both individual leaders and their subordinates. Participants noted that other substance abuse opportunities also surface as temptations in any military environment.

5. **Favouritism or Preferential Treatment.** Fairness is the cornerstone of effective command; however, our leaders made the case that the temptation to treat personnel by different or personally convenient standards was an issue that required attention and serious consideration. Though there may be rare reasons to justify this practice, "playing favourites" and related preferential treatment of personnel, for whatever reason, can create a variety of negative, unforeseen, and unpredictable problems in any command structure.

6. **"Blind Eye" and Failure to Report Wrongdoing.** The U.S. Army officer corps has a tradition of ethical behaviour starting with the West Point cadet honour code, which states that "a cadet will not lie, cheat, steal, or tolerate those who do." This same ethos is pervasive in every Service's formal ethical standards; however, in a highly competitive—and at times political—environment, participants noted that there may be incentives that could cause a leader to look away from or ignore wrongdoing. Whistleblowing has established processes and is encouraged across all the military branches, but participants made it clear that there exists a potential personal cost for engaging in this practice—one that might have a chilling effect on leaders, encouraging them to ignore a problematic situation.

7. **Exerting Inappropriate Influence on Personnel Decisions.** The U.S. military has well-defined standards and requirements for human resource decisions at all levels. Despite these established processes, participants stated that senior leaders can have a powerful influence on personnel processes for selection, promotion, and hiring decisions and, in some cases, can clearly overstep these stated guidelines. While leaders might, in their minds, have the best interest of the organization at heart, they can nonetheless override or unduly influence these established decision processes with potentially damaging and unforeseen negative side effects, as these activities do not take place in a vacuum.

8. **Offering/Accepting Gifts or Bribes or Quid Pro Quo.** Senior leaders have specific guidelines concerning offering or accepting gifts, yet virtually every focus group shared accounts of leaders being offered tickets to a sporting event or entertainment venue or a personal gift that was contrary to these strict guidelines. Participants agreed that this temptation is very real; they shared the belief that, the higher one rises in the organization, the greater the likelihood and frequency of this temptation. In addition, participants frequently tied quid pro quo to this discussion and it was frequently associated with a dialogue of how "transitioning to retirement" can open a potential hornet's nest of ethical questions, predicaments, and dilemmas.

9. **Hubris.** In a large and mission-driven enterprise, it is important that rules and the chain of command be followed. Yet participants stated that, in select circumstances, some officers might be tempted to knowingly violate policy or disobey an order if they believe doing so can provide them with a desired benefit or outcome. The keywords in these discussions were *knowingly* and *personal gain*. Participants discussed the temptation that exists when leaders erroneously believe that they are bigger than rules, policies, and regulations, which is frequently driven by unbridled ego, egocentrism, and hubris. And as an additional warning, they made it clear that the higher a leader rises in the organization, the greater this potential temptation.

10. **Seeking/Demanding Deference or Preferential Treatment.** Groups identified the issue of showing favoritism as a temptation of command. They also pointed out that if leaders are not careful, they can find themselves seeking or even demanding favoritism or special treatment as they navigate the military's large and complex operating systems. This temptation can come in many forms, including seeking perks, travel arrangements, and line jumping, among others. These actions are frequently driven by leaders' belief that the rules do not apply to them, as previously discussed, or the need for expediency.

In summary, these top ten potential temptations—moral and ethical challenges that leaders can face in senior military positions—are a challenge for *everyone*. All leaders face temptation, but the real question is whether they have the strength of character and moral courage to withstand those temptations and continue to do the right thing regardless of circumstance.

Source: Clinton Longenecker and James W. Shufelt, 'Conquering the Ethical Temptations of Command: Lessons from the Field Grades', National Defense University Press (31 March 2021), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2553439/conquering-the-ethical-temptations-of-command-lessons-from-the-field-grades

Annex II

Further adult learning theories[73]

Behaviourism

The theory of behaviourism, introduced by Watson and Skinner,[74] proposes that all learning is observable. In this view, assessing whether participants have learned something through training requires examining changes in their behaviour. Thus, learning becomes more effective and practices reinforced when activities are designed to allow participants to model new behaviours and receive immediate feedback.

Constructivism

The theory of constructivism posits that people build new ideas and concepts upon their existing knowledge and experiences, forming new connections and assigning fresh meanings. Consequently, both the experience itself and the way we interpret and explain it directly shape our learning. For this reason, facilitators should first identify participants' prior knowledge to effectively link it to newly introduced concepts.

Transformative learning

The goal of transformative learning is not merely to add new layers of knowledge but rather to reframe participants' perspectives. This approach encourages self-reflection and the questioning of previously held beliefs. Its main principles are:

- **Critical reflections** – re-examining the meanings individuals have previously attached to specific situations and assessing whether they remain relevant.
- **Reflective discourse** – engaging in open discussion with others and being open to alternative viewpoints to critically reflect on the new experiences to form revised judgements.

Holistic learning

This theory emphasizes the uniqueness of learning experiences, viewing each learner as a 'whole person' across intellectual, psychological, physical, and spiritual perspectives. Rather than compartmentalizing the learning process, it is important to educate individuals within a larger context which considers their societal environment. As training goals may differ for each person, the facilitator's role should be that of a guide. The theory rests on three key principles:

73 This section has been adapted from a training manual on police integrity published by DCAF in 2015: Paulo Costa and Isaline Thorens, Training Manual on Police Integrity (Geneva: DCAF, 20 December 2015), https://www.dcaf.ch/node/12922

74 John B. Watson and B.F. Skinner were both influential American psychologists who founded and developed the theory of behaviourism. Watson, considered the father of behaviourism, focused on how behaviour is shaped by external stimuli (classical conditioning), while Skinner expanded on this with operant conditioning, emphasizing the role of consequences (reinforcement and punishment) in shaping behaviour.

- **Balance** – ensuring the curriculum is balanced between traditional practices and spiritual, intuitive, and collaborative learning methods.
- **Inclusion** – encouraging learners to explore various methods and perspectives while avoiding discrimination based on educational orientation.
- **Connection** – emphasizing the relationship between people, experiences, and concepts rather than separating them into discrete categories.

Gagné's Conditions of Learning and Taxonomy[75]

Robert Mills Gagné formulated the theory of learning conditions and learning levels, outlining key factors that optimize the learning process. Although the theory has been applied in different spheres, it was initially focused on military training settings.

Gagné's five Conditions of Learning:

1. **Intellectual skills (Cognitive domain)** – the learner knows how to solve a problem through the application of the acquired knowledge.
2. **Verbal information (Cognitive domain)** – the learner can articulate, express, and explain the acquired new knowledge.
3. **Cognitive strategies (Cognitive domain)** – the learner cultivates strategies and thinking techniques to analyse problems and solve similar situations.
4. **Motor skills (Psycho-Motor domain)** – the learner can physically perform the taught actions required to solve a problem.
5. **Attitudes (Affective domain)** – the learner's mental state that influences and guides their choice of personal action.

Learning typically involves interactions across different domains, with the cognitive domain often being a pre-condition for learning in other areas. While ethics primarily focuses on attitudes and behaviours, it also encompasses elements of the cognitive domain, such as understanding laws, codes of conduct, and codes of ethics. Recognizing these aspects when designing effective learning strategies and outcomes is essential.[76]

In addition, Gagné developed nine Levels of Learning, which can be applied by facilitators to deliver training in a structured manner:[77]

1. **Gain Attention (reception).** Can be achieved through posing questions or using relevant stimuli.
2. **Inform Participants of the Objective (expectancy).** Adult learners need to clearly understand the goals they are expected to achieve to nurture their inner motivation.
3. **Stimulate Recall of Prior Knowledge (retrieval).** Activation of learners' existing knowledge facilitates the connection between new concepts and existing mental frameworks.
4. **Present the Content (selective perception).** The substance of the training should be structured, logically sequenced, and delivered through appropriate media.
5. **Provide Learning Guidance (semantic encoding).** Provide clear explanations and real-life examples to help participants grasp the content.

75 Costa and Thorens, Training Manual on Police Integrity; Jennifer Kretchmar, 'Gagné's Conditions of Learning', Research Starters: Religion and Philosophy, EBSCO Information Services (2023), https://www.ebsco.com/research-starters/religion-and-philosophy/gagnes-conditions-learning

76 Costa and Thorens, Training Manual on Police Integrity.

77 Saul McLeod, 'Gagné's Conditions of Learning Theory', Simply Psychology (updated 1 February 2024), https://www.simplypsychology.org/conditions-of-learning-gagne.html

6. **Elicit Performance (responding).** Give participants the opportunity to practise what they have acquired through hands-on activities.
7. **Provide Feedback (reinforcement).** Provide feedback on performance to enable participants to assess their progress and identify areas for improvement.
8. **Assess Performance (retrieval).** Use various assessment methods, such as quizzes, tests, or practical exercises to evaluate participants' progress.
9. **Enhance Retention and Transfer (generalization).** Provide participants with the opportunities to review acquired knowledge and apply it in real-world contexts that promote the transfer of knowledge across various domains.

Experiential learning[78]

Developed by David Kolb, this theory places experience at the centre of the learning process, following the principle of 'learning by doing'. Adults acquire new skills and strengthen their understanding when engaged in activities and reflection. The experiential learning cycle has four stages:

1. **Concrete experience** – learning something new or engaging with a familiar situation in a new way.
2. **Reflective observation** – thinking about and reflecting on that experience in light of existing knowledge.
3. **Abstract conceptualization** – making sense of experiences and reflections, and formulating solutions and plans for further action.
4. **Active experimentation** – applying insights and ideas in practice and observing how outcomes differ from initial experiences.

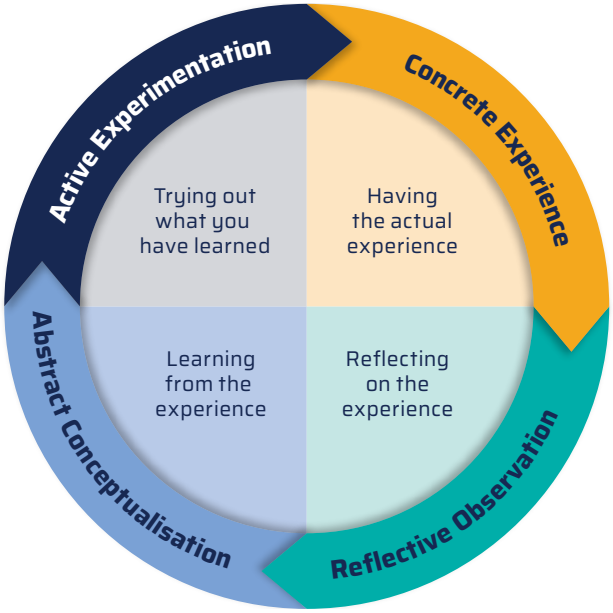

Figure 8. Kolb's Experiential Learning Cycle

Taken from: Saul McLeod, 'Kolb's Learning Styles and Experiential Learning Cycle, *Simply Psychology*, updated 19 March 2025 https://www.simplypsychology.org/learning-kolb.html

78 Irina Ketkin, 'A Comprehensive Guide to Adult Learning Theories', The L&D Academy (7 November 2023, updated 19 October 2024), https://www.theldacademy.com/post/a-comprehensive-guide-to-adult-learning-theories

Learning styles

Based on the learning cycle, Kolb developed four distinct learning styles, namely diverging, assimilating, converging, and accommodating. These are influenced by social environment, educational experiences, or basic cognitive structures of the individual. Preference for learning style is the product of two pairs of variables (as can be seen in the following matrix), and one cannot perform both variables on a single axis simultaneously (e.g. think and feel). Nevertheless, everyone responds to and needs the stimulus of all four types, depending on the situation.

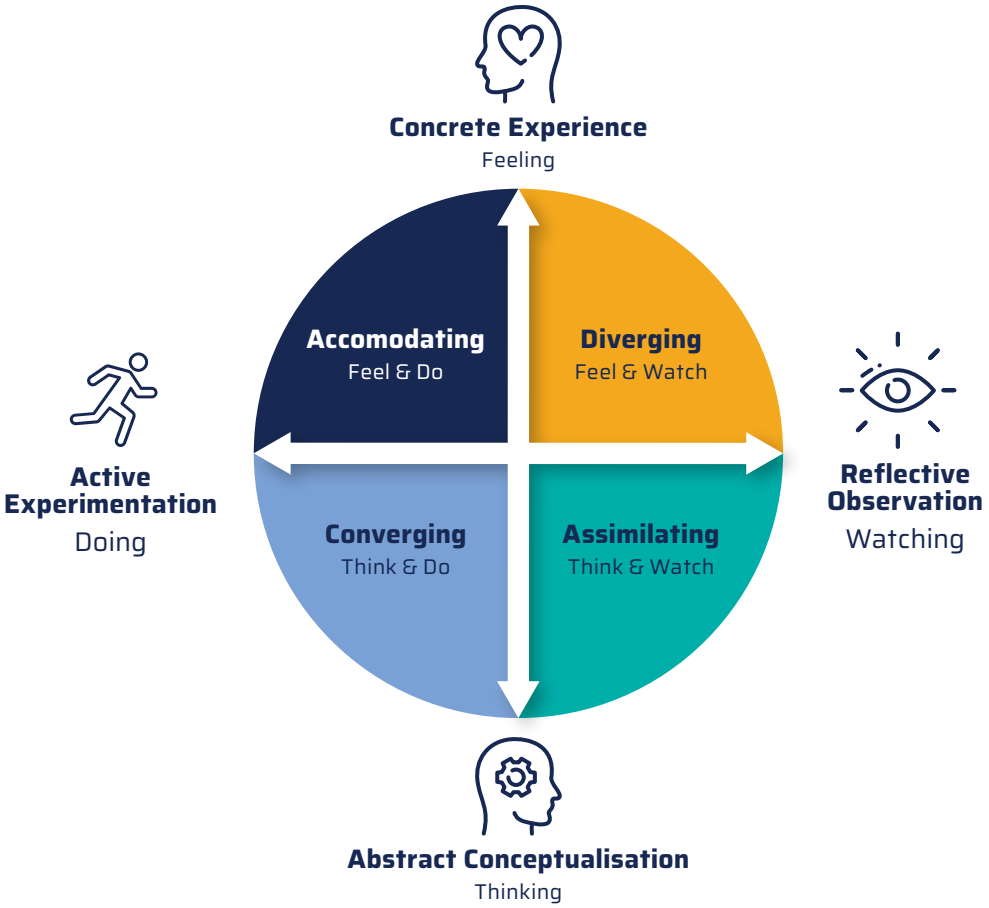

Figure 9. Kolb's Learning Styles

Taken from: Saul McLeod, 'Kolb's Learning Styles and Experiential Learning Cycle, *Simply Psychology*, updated 19 March 2025 https://www.simplypsychology.org/learning-kolb.html

Recognition that each individual has a unique learning style and preferred learning technique is crucial in designing training programmes. For example, some learners favour visual materials, such as images, graphs, and videos, while others are auditory and learn best through listening and discussion. Kinaesthetic learners, in contrast, engage through hands-on activities and a sense of touch.[79] When designing and delivering training, it is important to apply a methodology that combines various styles and activates all the senses, as this approach is most effective in catering for the different needs of people and accommodating varying attention spans.

79 Costa and Thorens, Training Manual on Police Integrity.

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

+41 (0) 22 730 94 00
info@dcaf.ch
www.dcaf.ch