NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD

DCAF Geneva Centre for Security Sector Governance

Building Integrity & Reducing Corruption in Defence



A Compendium of Best Practices

Volume II

Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices, Volume II

Brussels, Geneva, 2026

About NATO Building Integrity (BI)

The NATO Building Integrity (BI) Initiative was launched in 2007 by the Euro-Atlantic Partnership Council, with the primary goal to establish efficient and effective institutions that uphold the principles of integrity, transparency, and accountability. The BI Programme is committed to supporting NATO, Allies, and partner countries in promoting good governance and integrity within the defence and related security sector. NATO BI operates on the basis of mutual interest and goals, by providing country-specific support through tailored strategic advice and consultations, along with customized capacity building to strengthen national good governance. This includes strengthening defence institutions, developing their leadership, individual and institutional capabilities, and improving the processes and procedures for managing defence resources. It also encompasses an enhanced understanding of corruption as a threat to peace and stability, including in the context of NATO-led operations and missions, and as part of capacity-building efforts in non-permissive environments, such as military conflict zones.

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.

Chief editors: Prof. Todor Tagarev, Prof. David Whetham, Dr. Grazvydas Jasutis

Editorial board & institutional affiliations: Benedicte Borel (NATO IS), Dr. Nadja Milanova (NATO IS), Per Aage Christensen (CIDS), Dr. Grazvydas Jasutis (DCAF), Thomas Gooch (NATO SHAPE), Dr. Michael Ofori-Mensah (TI-DS), Rinske Fieten (COID), and Maj. Rudi van Eck (COID).

Contributors: Dr. Grazvydas Jasutis, Dr. Karolina MacLachlan, Alexandra Addison-Wrage, Prof. Todor Tagarev, Prof. Francois Melese, Dr. Nadja Milanova, Thomas Gooch, Damir Ahmetovic, Roman Rukomeda, Valeri Ratchev, Christopher Staudt, Francisco Cardona, Anela Duman, Teodora Fuior, Dr. Stephanie Trapnell, Matthew Steadman, Dr. Michael Ofori-Mensah, Denitsa Zhelyazkova, Dr. Erny Gillen, and Gen. Steve Thull.

Research support: Vlasta Kovbasa, Nikol Petkova, Richard Steyne, and Nino Shanshashvili.

Other contributions: Darko Stancic, Kristina Vezon, George Lucas, and Vassil Genchev.

NATO BI/Governance and Institutions Team coordinated the project: Benedicte Borel (2020–2023), Alice Wilhelmi (Jan.–Jun. 2022), Sophie Buddenhorn (Jan.–Jun. 2023), and Dr. Mihaela Racovita (2024–2026).

Copy-editor: Aravis Global Advisors
Graphics and Printing: NATO Printing & Graphics, Brussels, 2026; DCAF, Geneva, 2026
ISBN: 978-92-9222-827-9.

Note: Page numbers vary slightly between the printed and online version; please specify the version when citing.

Disclaimer: The views presented in this publication are the responsibility of their authors and do not represent the official views of NATO.

Funding: This study was possible due to the financial support of the Government of Switzerland, and the contributions of NATO and the BI Initiative of the NATO Partnership Trust Fund.

Foreword

The strategic landscape confronting NATO, its Allies and partners has rarely appeared as intricate, nor as persistently unsettled, as it does today. From the reverberations of Russia's war of aggression against Ukraine to the more discreet yet equally corrosive hybrid attempts to erode democratic processes in Moldova, the rules, institutions, and norms underpinning our collective security are subjected to continuous strain. In response to this evolving reality, Switzerland has worked alongside NATO and partner nations to reinforce the foundations of good governance through the Building Integrity Programme — an initiative designed to enhance the effectiveness, efficiency, and resilience of defence and related security institutions. Experience has repeatedly demonstrated that corruption and fragile governance structures squander scarce resources, diminish operational performance, and ultimately weaken public confidence. At a time when defence expenditure is rising to meet mounting challenges, safeguarding these investments through credible oversight remains indispensable.

Anchored in the enduring principles of transparency, integrity, and accountability, NATO, Allies, and partners have steadily exchanged best practices, confronted structural shortcomings, and explored emerging dilemmas born of military operations in complex security environments. This collaborative endeavor reflects a shared recognition that resilience is not merely a function of capability, but of trust — trust within institutions and trust between them. Within this framework, Switzerland's commitment has been both consistent and substantive. The present second volume of the NATO Building Integrity Compendium of Best Practices draws upon nearly two decades of accumulated experience since the Programme's inception and builds upon the first volume published in 2010 with Swiss support. Beyond political and financial engagement, Switzerland's contribution is enriched by the expertise of the Geneva Centres — DCAF, GCSP, and GICHD — whose work continues to bridge policy, practice, and innovation. The year 2026 also marks the anniversary of Switzerland's accession to the Partnership for Peace, a milestone that initiated a steady deepening of relations with NATO and was accompanied, notably in 1996, by the establishment of these three Geneva-based institutions. Today, this legacy underscores the enduring relevance of the values that bind our cooperation with NATO.

Finally, I wish to convey my sincere gratitude to all Allies and partner nations whose dedication, knowledge, and collaborative spirit have shaped this important undertaking. Strengthening integrity and good governance in the defence and security sector remains demanding work. Yet by openly sharing both our successes and our challenges, we improve together — and it is this spirit of cooperation that gives this Compendium its real value in uncertain times.

Ambassador Jacques-H. Pitteloud

Head of the Swiss Mission to NATO

Acknowledgments

This valuable work was made possible through the commitment and contribution of numerous experts, researchers, and practitioners, who have consented to share their knowledge and experiences, for the benefit of all. The idea behind the NATO Building Integrity Compendium was, from the very beginning, to collect and to share emerging best practices, and promising solutions to tackle the complex challenges posed by corruption and poor governance in the defence and related security sector.

The first volume of the NATO Building Integrity (BI) Compendium of Best Practices was published in 2010, and since then it has been widely requested, read, and utilized – a testimony to its high quality and usefulness. It has since been published in English and French, and in other 12 languages, including: Arabic, Romanian, and Ukrainian.

This second volume of the NATO BI Compendium emerged from a need to take stock of new lessons and emerging best practices which were needed to navigate the profound changes in the political and security landscape in the transatlantic area over the past 15 years. The BI Compendium provides information and analysis on BI best practices to national institutions of the defence and related security sector of Allied and partner countries, and is also a practical tool to support the strengthening of defence and security institutions and processes.

The process of elaborating this second volume of the BI Compendium has in itself been complex. The volume benefitted from the early support of an Editorial Board composed of: NATO IS, SHAPE, the Centre for Integrity in the Defence Sector of the Ministry of Defence of Norway (CIDS), the Geneva Centre for Security Sector Governance (DCAF), the Central Organisation Integrity Defence (COID) of the Dutch Ministry of Defence, the Defence & Security programme of Transparency International UK (TI-DS), and others. These institutions and their experts contributed to the development of the core content. And in 2025, DCAF agreed to take on the role of finalizing this second volume, and putting it over the finish line.

We gratefully acknowledge the valuable contributions of all the: authors, co-authors, reviewers, editors, copy-editors, project assistants, designers, and all other supporters who have made this second volume a reality.

We also gratefully acknowledge Switzerland's financial support in bringing this project to fruition, as well as all other contributions to the BI Initiative of the NATO Partnership Trust Fund. Past experience has shown that an essential component of the work of NATO BI consists in the promotion of national experiences and expertise, and the sharing of lessons identified and/or learned, within the NATO BI Community of Practice, and across national defence and related security institutions. This Volume is an important contribution to that work, and to the strengthening of our collective security.

The NATO Governance and Institutions Team
International Staff, Operations Division, NATO HQ

Editorial Preface

In 2010, NATO and the Geneva Centre for Security Sector Governance (DCAF) published the first repository of best practices in *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices*. This volume builds on the accumulated experience in implementing NATO's Building Integrity (BI) programme. It treats persistent and new challenges in a comprehensive manner. Researchers and practitioners from international, governmental and non-governmental organizations share their experience and knowledge here on the most salient defence integrity issues.

The volume is the outcome of a pro-active hard-working intellectual coalition. Its chapters reflect dynamic cooperation between NATO practitioners, civil society, academic researchers, and defence professionals working at the intersection of theory and practice. This shared endeavour has produced a toolkit that is both rigorous and operationally relevant. It combines conceptual insight, tested expertise, and evidence collected by experts. The Compendium demonstrates that when institutions, scholars, and civic actors work together, they can generate knowledge beneficial for informing policy-makers, shaping strategy, and strengthening democratic governance in the defence sector.

The impetus for this collaboration did not arise in isolation. It was prompted by the disruptions affecting today's security environment. Russia's war against Ukraine, rising transactional politics, hybrid attacks on democratic systems, and corruption used as a geopolitical weapon required an intellectual response. NATO member states and partners have learned the hard way that poorly governed defence sectors are vulnerable. The Compendium was therefore inspired by this practical need, the need for a better understanding of corruption risks in defence and equipping Allies, partners, and institutions, with tools to prevent integrity failures that weaken security.

At the same time, this Compendium advances integrity building in new ways. It expands beyond traditional anti-corruption framing. It links integrity with human security, resilience, hybrid threats, mission effectiveness, institutional culture, and democratic oversight. It includes fresh empirical analysis, methodological innovations, and case studies illustrating how values-based leadership, risk assessments, oversight, and organizational education shape institutional performance. It reframes integrity not as a compliance toolkit but as a strategic asset. It contributes to the core NATO tasks: deterrence and defence, crisis prevention and management, and cooperative security.

It also tackles an intellectual challenge and offers a holistic reflection on what integrity means in the twenty-first century. It demonstrates that building integrity is no longer a niche agenda. It is a discipline driven by partnerships, and enriched by new perspectives that bridge governance, human rights, culture, security studies, and military practice.

This Compendium is therefore both a product and a guidepost. It is a product of collaboration across communities of practice and knowledge. It is a guidepost ushering towards the future of integrity studies. It invites scholars, policymakers, and practitioners alike to continue the conversation, deepen the cooperation, and pursue integrity as a pillar of defence effectiveness and democratic resilience.

Table of Contents

Foreword 3

Acknowledgments 4

Editorial Preface 5

Introduction: From Building Integrity to Strengthening Good Governance 8

Part 1: The Corruption Challenge 13

1. The Impact of Corruption on Defence 14
2. Corruption as a Weapon in the Modern Hybrid-Influence Toolbox 22
3. The Impact of Human Rights Violations on Operations 32

Part 2: The Comprehensive Approach to Building Integrity 43

4. A Strategic Approach for Improving Defence Integrity: Legal, Ethical, and Governance Perspectives 44
5. The Evolution of NATO's Strategic Approach to Integrity and Good Governance in the Defence and Related Security Sector 56
6. NATO's Military Concept for Building Integrity in Operations 67

Part 3: Corruption Risks and Good Practices in Defence 76

7. Human Resource Management 77
8. From S.E.A.L. to SALE – The Importance of Human-Centric Military Career Transition for Diminishing Integrity Challenges in the Defence and Security Sector and in Society 96
9. Risks: Budgeting and Financial Management 110
10. Integrity in Defence Procurement 118
11. Benefits and Risks of Military Public-Private Partnerships (PPPs) 130

Part 4: Players in Building Integrity 138

12. Parliaments: Using the Power of the Purse in Tackling Defence Corruption 139
13. Anti-Corruption Agencies 152
14. Civil Society and Defence Institutions 162

Part 5: Organizing Building Integrity Initiatives 175

15. Mapping Corruption Risks 176
16. Building Integrity Programmes 187

Case Study: A Values Charter in the Luxembourg Armed Forces 198

List of Boxes

Box 2.1. Russia Continues to Use Corruption to Influence Ukraine's Politics, Undermining International Support 26
Box 2.2. Russia Uses Corrupt Networks to Sway Elections in Moldova 27
Box 2.3. Russia's Hybrid Influence in the Sahel 28
Box 3.1. The Approach of NATO to Preventing and Responding to Sexual Exploitation and Abuse 36
Box 3.2. Good practice: NATO Policy for the Protection of Civilians 38
Box 4.1 Examples of Corruption – 'the Misuse of Public Office for Private Gain' 47
Box 4.2. Examples of Enhancing Transparency Measures in Budgeting and Procurement 47
Box 4.3. Investments to Minimize Corruption 48
Box 4.4. Checks and Balances in Internal MoD Decision-Making 53
Box 5.1. NATO BI Self-Assessment and Peer Review (NATO BI Process) 62
Box 6.1. Waste and Corruption in Supporting Local Forces and Economies: Examples from Afghanistan 70
Box 6.2. Impact of Corruption on Public Perceptions and the Desired End State 71
Box 7.1. Examples of HRM-related Corruption and Impact 78
Box 7.2. Example of Good HRM Practice: Selection of Public Servants in Albania 85
Box 7.3. Good HRM Practice: BITEC's e-Learning Training System in Ukraine 91
Box 7.4. Good HRM Practice: Assessing the Risk of Corruption at Individual Work Posts. 93
Box 8.1. Typical "Good Practices" in Building a Military Career Transition System 97
Box 8.2. Health Care Provided to U.S. Eligible Veterans 104
Box 8.3. The UK Strategy for Veterans 2018–2028 105
Box 8.4. Good Practices in Providing Effective and Honest Military Career Transition 106
Box 10.1. Main Corruption Risks in Defence Procurement 119
Box 10.2. Integrity Principles of the Organisation for Economic Co-operation and Development 121
Box 10.3. Impact of EU Procurement Directives on Integrity 122
Box 10.4. Speeding Up Drone Delivery 125
Box 10.5. Reforming Ukraine's Defence Procurement System 126
Box 10.6. The Role of CSOs in Strengthening Transparency in Defence Procurement 127
Box 11.1: Dutch Case Study 131
Box 11.2: Military Housing PPP Case Study 133
Box 12.1: Black Budgets in the United States 142
Box 12.2. What Does the Term 'Defence Budget' Stand for? 143
Box 12.3. Parliament Involvement in Budget Formulation 147
Box 12.4. Methods to Determine Annual Expenditures for a Ministry 147
Box 12.5. What Are the Consequences of the State Budget being a Law? 148
Box 13.1. Closing Down an ACA for Political Reasons: The Case of Portugal 156
Box 13.2. Examples of ACAs' Activities in the Defence and Security Sector 159
Box 15.1: Key Roles in Assessing Corruption Risks 179
Box 15.2: Risk Assessment Tool Impact: GDI 183
Box 16.1. Good Practices in BI Design Using the Example of Bosnia and Herzegovina 191
Box 16.2. Proposed Defence Performance Management Framework 194
Box 16.3. Communication 195

Introduction: From Building Integrity to Strengthening Good Governance

Dr. Grazvydas Jasutis

NATO's Building Integrity initiative (NATO BI) emerged as part of NATO's commitment to promoting good governance and reducing corruption within the defence and security sectors of its member and partner countries. In 2010, the First NATO BI Compendium edited by Prof. Todor Tagarev was launched. It addressed corruption risks in NATO member armed forces such as opaque personnel policies, procurement, and military involvement in economic activities, emphasizing the need for ethical standards, transparency, and accountability through legal frameworks, independent oversight, and sustained leadership.

Since its inception, the NATO BI programme has grown in both scope and significance, mirroring NATO's geographic and political enlargement. As the Alliance has welcomed new members, particularly from Eastern and Central Europe and the Western Balkans, the NATO BI initiative has adapted to support these states in strengthening anti-corruption mechanisms and embedding international best practices into defence institutions. NATO advanced its BI initiative through tools like the Self-Assessment Questionnaire, Peer Review Process, and SME pool; expanded participation for Allies and partners; formalized BI at the 2014 Wales and 2016 Warsaw Summits with a policy, action plan, curriculum, and online course; and launched a Trust Fund supported by Norway, Switzerland, the UK, and the EU to strengthen integrity-building cooperation.[1]

NATO BI has come to serve not only as a technical assistance programme but also as a platform for dialogue, peer learning, and capacity-building, helping to align the security sector reform efforts of partner and aspiring member states with NATO standards of security sector governance.[2] In light of these developments, NATO recognized the need to formalize the lessons learned and emerging challenges through an updated policy framework. As a result, the decision to develop a second volume of the BI Compendium was taken, and work on the second Compendium began in 2021.

The war in Ukraine challenged and further catalysed the transformation of BI. It has profoundly influenced political discourse, particularly by introducing the public and political use of military terminology. Terms like 'Javelins', 'HIMARS', 'Stingers', 'NASAMS' and other types of advanced weaponry used by the Ukrainian Armed Forces have become part of the everyday vocabulary of politicians, media commentators and even ordinary citizens. Military hardware has increasingly become a symbol of solidarity, deterrence, and strategic commitment. As military aid, increases of defence budgets and operational concerns dominate policy agendas, the foundational principles of SSG risk being overshadowed. The war in Ukraine has triggered a substantial increase in BI programme activities. Nevertheless, there is still limited clarity regarding their concrete outcomes and measurable impact. Even based on the comparison of NATO summit declarations, a discourse analysis reveals an evolving shift in NATO's official language from value-driven governance to hard security, especially in the aftermath of major geopolitical events. Partly, the variables of resilience and human security might compensate. As an official NATO concept, resilience can perhaps bridge the gap between value-driven governance and hard security, considering it is defined as 'the individual and collective capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions, and to ensure the continuity of the Alliance's activities'.[3] In addition, the concept of human security can also work as a bridge between more principled considerations and security-centred approaches (with its five different areas: combatting trafficking in human

[1] NATO, *Building Integrity in Operations: A Toolkit for NATO,* https://shape.nato.int/resources/3/website/building_integrity_toolkit.pdf; NATO, "Wales Summit Declaration," September 5, 2014, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration (accessed February 23, 2026).
[2] DCAF, *Security Sector Governance: Applying the Principles of Good Governance to the Security Sector* (Geneva: DCAF, 2015), https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_1_Security_Sector_Governance_EN.pdf.
[3] NATO, "Resilience, civil preparedness and Article 3," November 13, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3 (accessed February 23, 2026).

beings; protection of children in armed conflict; preventing and responding to conflict-related sexual violence; protection of civilians; and cultural property protection).[4]

This requires reinforcing the need for the integration of BI and good governance principles in building long-term institutional integrity, public trust, and state legitimacy. A base for this is the premise that the overall security of the state fundamentally relies on the dedication, integrity, courage, and professional competence of each individual serving within its security institutions and that individual's respect for human rights. It is of no consequence whether these individuals serve in the military, domestic security services, or international peacekeeping. Individual shortcomings, such as incompetence or corruption, and the absence of appropriate professional education and training, significantly undermine the effective and ethical performance of their duties. These visible weaknesses, however, are often the manifestations of deeper, more nuanced issues within the broader security culture. At the core of a resilient and trustworthy security apparatus lies not only technical skill and compliance with regulations, but also the cultivation of an ethical security orientation.[5] This orientation encompasses an internalized commitment to democratic values, personal accountability, and an understanding of security as a service to the public rather than as an instrument of unchecked power. Without systematically nurturing these subtler dimensions through leadership, continuous education, institutional ethics programs, and societal engagement, the state risks weakening the very foundations of its security institutions. Thus, the integrity of the entire security system is inseparably linked to the moral and professional strength of its individual members, supported by a broader environment that prioritizes transparency, accountability, and respect for human rights.[6]

The second NATO BI Compendium builds on the 2010 Compendium. It offers a more strategic, operationally integrated, and future-focused framework for integrity in the defence sector. It positions BI not just as a governance tool, but as a critical element of NATO's collective resilience and mission success in an increasingly complex security environment. It recognizes that the wider impact of NATO BI initiatives promotes an overall emphasis on good governance, rule of law, and respect for human rights generally. The second Compendium reflects recent experience and shifts in the global security landscape. It moves beyond awareness and capacity building toward operational integration (also known as interoperability), hybrid threat response, and holistic governance. There are significant advantages that improve the conceptual basis of integrity and make it more operational.

First, the second Compendium provides **an augmented perception** of the concept. It significantly advances the conceptual understanding of corruption by framing it not merely as a governance issue but as a direct security threat. It recognizes that corruption undermines operational effectiveness, erodes institutional trust, and can be weaponized in the context of hybrid warfare. For instance, the article 'Corruption as a Weapon in the Hybrid Influence Toolbox' examines how Russia and China have redefined warfare by incorporating corruption into their hybrid influence strategies. Corruption is used as a weapon to weaken state institutions, compromise officials, and destabilize societies while avoiding open conflict. The article goes on to detail historical evolutions from Cold War tactics to modern-day hybrid warfare and highlights how corruption, once a covert tool, is now openly deployed against the West to erode governance, trust, and stability. The article 'The Impact of Corruption on Defence' highlights how corruption wastes resources, fuels violence, weakens military readiness, and undermines international peace efforts. By explicitly linking the BI agenda to operational outcomes and resilience against hybrid threats, the Compendium strengthens the strategic relevance of anti-corruption efforts within broader security and defence planning. Addressing corruption is positioned as an essential element in safeguarding national and allied security.

---

[4] NATO, "Human security," August 30, 2024, https://www.nato.int/en/what-we-do/wider-activities/human-security (accessed February 23, 2026).

[5] George R. Lucas Jr., Dragan Lozancic, Grazvydas Jasutis, et al., *Conceptualizing the Relationship of Good Security Sector Governance to the State Security System* (Geneva: DCAF, 2022), https://www.dcaf.ch/sites/default/files/publications/documents/RelationshipGoodSecuritySectorGovernanceStateSecuritySystem_EN.pdf.

[6] Ibid.

Second, the Compendium captures **much broader governance** perspectives. The Compendium moves beyond a narrow anti-corruption focus to embrace a wider governance lens. It underscores the importance of values-based leadership, societal trust, and human-centric approaches to security sector reform. This broader framing acknowledges that integrity must be deeply embedded in leadership practices and institutional culture to ensure sustainable, long-term resilience. This can be seen clearly in the 'Case Study: Luxembourg Armed Forces' Values Charter.' The Luxembourg Armed Forces developed a new Values Charter and Military Code of Conduct through a collaborative, participatory process involving the Ministry of Defence, military leadership, and an ethics expert. The initiative emphasized embedding values into military identity and operations, reflecting the diversity of Luxembourg's multicultural society. New trends are emphasized in the article 'Human Resource Management for Building Integrity.' It argues that effective Human Resource Management (HRM) is vital for building integrity within defence institutions. It outlines good practices for planning, recruitment, performance management, and professional development, drawing on international standards. HRM should support an ethical culture, minimize corruption risks, and align military HRM practices to civilian public service norms while retaining necessary military specifics. The broader governance aspects are well captured by the article 'Military-to-Civilian Transition and Integrity Risks.' The transition of military personnel to civilian life is a complex process critical for personal well-being and national security. Poorly managed transitions can create integrity risks such as corruption, marginalization, or criminal involvement. A human-centric Military Career Transition system supports service members before, during, and after leaving the military, ensuring they adapt successfully. Best practices emphasize early preparation, public support, inter-agency cooperation, and protecting veterans' dignity while integrating them into civilian society.

Needless to say, civil society plays a pivotal role in strengthening defence governance by enhancing transparency, oversight, and accountability. Historically excluded from defence decision-making, civil society organizations (CSOs) now advocate for reform, provide expertise, facilitate dialogue, monitor government actions, and sometimes even help implement programs. Using tools like the Government Defence Integrity Index, CSOs assess integrity risks and civic space in NATO countries. Their engagement as mentioned in the article 'Civil Society and Defence Institutions' is essential for democratizing defence governance and for building societal trust.

Third, the new Compendium focuses more on **operational realities**. Recognizing the realities of today's security environment, the second Compendium provides practical guidance on how to integrate Building Integrity principles into military operations, including during mission planning, execution, and post-mission evaluation. This operational focus ensures that integrity is treated not as an abstract principle but as a functional enabler of mission success and as a force multiplier too. The article 'Building Integrity in Operations (NATO Military Concept)' states that NATO's 2021 Military Concept for Building Integrity in Operations (BIIO) addresses corruption as a key risk undermining operational success. The concept introduces principles of integrity, transparency, and accountability in military operations and offers a practical framework (Understand, Plan, Execute, Assess) for addressing corruption risks. Case studies from Afghanistan reveal how endemic corruption contributed to mission failures, emphasizing the need to integrate anti-corruption measures into operational planning and execution. The article 'Human Rights Violations and Their Impact on Military Operations' explains how human rights violations during military operations can damage operational effectiveness, credibility, and mission success. It examines how abuses, such as torture, illegal detention, and sexual violence create corruption risks, alienate local communities, and fuel insurgencies. It stresses that integrating human rights protections into military operations is essential for maintaining legitimacy, securing local support, and ensuring mission sustainability.

The Compendium also looks into the topics that directly impact operations – such as defence procurement and defence budget. The article 'Building Integrity in Defence Procurement' underlines that defence procurement remains highly vulnerable to corruption. Though transparency and competition have improved, open competition is still rare. Many contracts are awarded through non-transparent procedures. Strengthening oversight, applying OECD principles, and fostering competition are recommended to reduce corruption risks and enhance public trust in defence procurement. Similarly, the article 'Risks: Budgeting and Financial Management' discusses how public expenditure, especially in defence, is vulnerable to corruption. It emphasizes the

importance of transparent budgeting and strong financial controls. International instruments like the UN Reporting Instrument and OECD Best Practices promote transparency, while opaque defence budgets increase risks of misuse, weaken public trust, and harm security governance.

Fourth, the new Compendium explores **some innovative themes**. The article 'Evolution of NATO's Strategic Approach to Integrity and Good Governance in the Defence and Related Security Sector' underlines that integrity development has been integrated within the context of NATO's wider policy objectives and the implementation of the Alliance's core tasks. The development of effective, transparent and accountable defence institutions, which are responsive to unpredictable security challenges, including those of a hybrid nature, contribute to the fulfilment of the Alliance's mission. The Compendium explores emerging areas critical to contemporary defence governance, such as the management of public-private partnerships (PPPs), transitions in defence human resources, and reforms grounded in military values. For instance, the article 'Public-Private Partnerships in the Defence Sector' emphasizes that PPPs are increasingly used in defence to improve innovation and cost-efficiency. While PPPs offer benefits like faster technology adoption and resource optimization, they also introduce significant integrity risks, such as conflicts of interest, information asymmetry, and renegotiation vulnerabilities. The article stresses the need for rigorous risk assessments, transparency, and accountability mechanisms to ensure PPPs strengthen, rather than undermine, defence capabilities. It is not the only novelty in the Compendium. Viewing veterans' reintegration as an integrity issue (not just a social support question) is a novel argument. Poorly managed transitions create risks for corruption, societal instability, and even security threats. Emphasizing practical, field-driven BI tools, stressing the importance of civil society, parliaments, and the international community in sustaining reforms, and bringing human rights and operational aspects of integrity to the spotlight adds new added value to the concept. Integrating BI considerations into mission planning and operations (e.g. NATO's BI in Operations Concept) shows a shift from theoretical frameworks to practical applications in the field.

Fifth, it clearly promotes **institutional synergy**. A key strength of the Compendium is its emphasis on a comprehensive governance approach that ties together the efforts of the military, civil society, oversight bodies, and parliaments. This interconnected strategy reinforces institutional synergy, recognizing that genuine reforms require coordinated action across all pillars of democratic governance. Parliaments play a crucial role in ensuring integrity in the defence sector through budgetary control ('the power of the purse'). Despite challenges like information asymmetry with the executive, parliaments must prioritize defence integrity because corruption undermines security, wastes public funds, and damages public trust. Defence budgets, often opaque due to secrecy or complex structures (e.g. off-budget expenditure), require rigorous oversight. Special attention is needed to manage classified expenditures ("black budgets") and ensure transparency without compromising national security. The article 'The Role of Anti-corruption Agencies' states that the internationalization of anti-corruption efforts has led to the creation of numerous Anti-corruption Agencies (ACAs), influenced by instruments like the UN Convention against Corruption (UNCAC) and the OECD Anti-Bribery Convention. ACAs vary widely but should be independent, specialized, and adequately resourced to function effectively. They coordinate national anti-corruption efforts, engage in prevention, and sometimes prosecute corruption. Their design critically affects their success. International standards emphasize functional independence to shield ACAs from political interference and ensure credibility. By synergizing the activities, it ensures that BI remains adaptable and relevant to the evolving needs of security institutions.

Finally, the Compendium is made to be applicable to **wider contexts.** The insights and recommendations found there are not confined to NATO member states. They are highly applicable to partner countries undergoing democratic transitions, recovering from conflict, or rebuilding national institutions. The article 'Designing and Implementing Building Integrity Programmes' offers insights into successful integrity reforms in the defence sector that require structured BI programmes integrated into institutional governance. Following principles of good governance (transparency, accountability, participation) and quality management (customer focus, leadership, continuous improvement), BI programmes help organizations address corruption systematically. Key steps include setting clear goals, measuring performance, engaging stakeholders, and ensuring leadership commitment. Effective BI programmes balance short-term reforms with long-term organizational culture change.

Understanding and mapping corruption risks are critical for effective integrity-building in defence sectors. Corruption risk is the vulnerability within systems that facilitates corrupt practices. Risk assessments should be methodical, using approaches like public perception surveys, expert evaluations, and case studies. Tools like Transparency International's Government Defence Integrity Index help identify high-risk areas and prioritize reforms. In this way, the Compendium supports a broader international agenda for stability, good governance, and security sector reform.

Across the Compendium, a consistent message emerges: building integrity in the defence sector is essential to national security, democratic resilience, and public trust. The articles collectively argue that corruption in defence is not just a financial or ethical issue. It directly threatens operational effectiveness, political stability, and international security cooperation. Together, the articles offer a comprehensive roadmap for contemporary defence governance reforms. They propose moving from isolated anti-corruption initiatives to integrated, cross-sectoral strategies that align military effectiveness, democratic governance, and societal trust.

Part 1: The Corruption Challenge

This section of the publication explores how corruption, hybrid influence, and human rights violations intersect with defence and security. The first article examines corruption as a core security challenge, explaining how it drains national resources, fuels instability, weakens militaries, and undermines international missions. The second article reveals how states such as Russia and China have weaponized corruption as part of hybrid warfare, using bribery, influence networks, and strategic manipulation to destabilize rivals and advance geopolitical goals. Here, corruption operates as a subtle but potent form of warfare capable of reshaping borders, alliances, and political outcomes. Finally, the third article turns to human rights in operations. It examines how violations of fundamental rights whether through civilian harm, abusive detention practices, or sexual exploitation can compromise the missions. Violations of human rights do more than harm victims; they fuel insurgency, erode trust, reinforces corruption, and sometimes push communities into the arms of adversaries. Therefore, human rights are considered not as abstract ideas but as operational imperatives. This part of the Compendium underlines that integrity, accountability, and respect for rights are strategic necessities for modern defence institutions.

1. The Impact of Corruption on Defence

Dr. Karolina MacLachlan[1]

Introduction

It is widely recognized that corruption, defined as the abuse of entrusted power for private gain, has a detrimental impact on economic development, political cohesion, and societies' ability to handle grievances and reconcile conflicting agendas and interests. Corrupt practices can exacerbate inequality, fuel a sense of exclusion for whole groups, increase state fragility, and diminish the legitimacy and effectiveness of governments.[2] Estimates put the cost of bribery – only one type of corrupt practices – at around USD 1.5 trillion, about 2% of the world's GDP, and peg corruption-related losses in developing countries at USD 1.26 trillion per year.[3]

Corruption can impact any sector, but it tends to thrive in environments where an abundance of resources meets individual discretion in decision-making and a lack of transparency. This makes the defence sector, with greater levels of secrecy, highly concentrated decision-making, more limited oversight, and a high degree of complexity, especially vulnerable to large-scale corrupt practices. One classic analysis has found that higher perceived levels of corruption are associated with higher defence expenditures as a share of both GDP and government expenditure; another estimated that corruption in arms trade, a key item in many countries' defence expenditures, may account for up to half of corrupt transactions in legal trade overall.[4] Defence consistently appears among the sectors considered high-risk for corruption, and defence procurement has been rated as affected by higher corruption risks than procurement in other sectors of government activity.[5] Defence corruption has affected all countries, from those struggling with conflict and development to those topping development and anti-corruption indexes.

The current security environment, shaped by Russia's full-scale invasion of Ukraine on 24 February 2022, has seen global and especially European military budgets rise significantly. In 2024, global defence expenditures reached USD 2.7 trillion, an augmentation of over 9% in real terms over 2023. Europe and the Middle East drove the increases, with all NATO members upping their budgets. NATO frontline states have been investing heavily in preparedness against a potential clash with Russia: Poland's defence budget, for example, has reached 4.2% of GDP.[6] At the 2025 summit in the Hague, almost all NATO Allies committed to raising defence and security spending to 5% of GDP by 2035, with 3.5% ringfenced for 'core defence requirements' and 1.5% directed toward critical infrastructure, national resilience, and development of the defence industrial base.[7] Demand for weapons, equipment and ammunition has increased exponentially, putting pressure on producers and supply chains, and potentially creating the incentives to cut corners. As NATO countries look to arms exports to help

[1] The chapter was written for Transparency International, Defence & Security.

[2] For a recent review of the effects of corruption, see Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, *Anti-Corruption in Fragile Settings: A Review of the Evidence*, (Bonn: GIZ, September 2020) https://www.giz.de/de/downloads/giz2020_en_anti-corruption_in_fragile_states.pdf.

[3] United Nations Office on Drugs and Crime (UNODC), Organisation for Economic Co-operation and Development (OECD), and World Bank, *The Impact of Corruption on Sustainable Development. Think piece by UNODC, OECD and World Bank for the G20 Anticorruption Working Group*, 2020, pp. 3,6, https://www.unodc.org/corruption/uploads/documents/Corruption_sustainable_development_C.pdf.

[4] Sanjeev Gupta, Luiz de Mello, and Raju Sharan, "Corruption and Military Spending," *IMF Working Paper*, 2000, https://www.imf.org/external/pubs/ft/wp/2000/wp0023.pdf; Joe Roeber, "Hard-Wired for Corruption," *Prospect Magazine*, August 27, 2005, https://www.prospectmagazine.co.uk/essays/56912/hard-wired-for-corruption (accessed February 23, 2026); Anna Persson, Mark Worth, and Petra Jeney, *High-Risk Areas of Corruption in the EU: A mapping and in-depth analysis*, (Brussels: European Commission, 2024).

[5] Agnes Czibik, Mihaly Fazekas, Alfredo Hernandez Sanchez, and Johannes Wachs, "Networked Corruption Risks in European Defense Procurement," in *Corruption Networks. Understanding Complex Systems,* ed. Granados, O.M., Nicolás-Carlock, J.R. (Springer, 2021), https://doi.org/10.1007/978-3-030-81484-7_5.

[6] Stockholm International Peace Research Institute (SIPRI), "Unprecedented rise in global military expenditure as European and Middle East spending surges," April 28, 2025, https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges (accessed February 23, 2026).

[7] NATO, "The Hague Summit Declaration," June 25, 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration (accessed February 23, 2026).

keep production lines open and lower prices, concerns about exports to markets where corruption has previously been a key issue resurface.[8] Major arms producers, exporters and importers alike display shortcomings in the governance of the defence sector: Transparency International's 2020 Government Defence Integrity Index (GDI) analysed corruption risk and institutional anti-corruption safeguards in the defence sectors of 86 countries, concluding that 35 countries assessed were at 'critical' or 'very high' defence corruption risk, and only one had 'very low' risk levels.[9]

Governments and defence institutions are thus facing an environment where greater availability of resources increases incentives and opportunities for corruption and the emphasis on quick improvements in preparedness might overshadow governance and institutional concerns. Yet decision-makers ignore institutional resilience, corruption and governance at their peril, since the conduct and governance of defence sectors can have an outsize impact on security and stability. As the remainder of this chapter will show, defence corruption can contribute to the outbreak and recurrence of conflict by channelling resources to narrow, particularistic networks; by undermining peace settlements; and by affecting international peace support operations. By wasting resources and undermining the integrity and morale of defence institutions, corrupt practices make it more difficult for states to respond to insecurity, violence and conflict; corruption can thus deprive countries of their last bulwark of defence when they most need it. By contributing to the diversion of weapons, corrupt practices provide terrorist organizations, militia, and organized crime groups with the means to continue fighting, exacerbating insecurity and violence that directly affect civilians. Finally, as discussed in another chapter in this volume, corruption is a tool of hybrid warfare, used by authoritarian states to influence defence, foreign and economic policy outcomes in other countries.

Defence Corruption and the Cycle of Conflict: Endangering Peace, Enabling Conflict

Corruption and conflict are frequent bedfellows: countries struggling with conflict and insecurity tend to have higher perceived corruption levels as well as higher defence corruption risks.[10] In societies composed of multiple ethnic, social, or identity-based groups, corruption has the potential to exacerbate societal divisions if it limits access to state resources or political representation for a particular group. If geared towards benefiting a specific group, corruption prevents the creation of mechanisms distributing benefits more evenly throughout societies.[11] In countries where state institutions have been captured by corrupt networks and repurposed towards extracting income benefiting narrow groups – a phenomenon known as state capture – corruption becomes more than a deviation from a workable governance system; it becomes the system. Its impact and prevalence appear to contribute to the outbreak of violent conflict: one study found a correlation between levels of corruption and levels of peace, and identified a 'tipping point' at which small increases in corruption prompted large increases in violence.[12] Perception of corruption in state institutions and of political exclusion is a key grievance contributing to the emergence of extremist groups and can be used to augment their appeal and their recruitment strategies. In Mali, for example, extremist groups prevalent in the country's northern regions vocally criticize government corruption and the military's abuse of civilians, presenting themselves as more

[8] The UK, for example, is planning to sell BAE-produced Tempest and Typhoon aircraft to, among others, Saudi Arabia and Qatar, where both BAE and the UK MoD have been implicated in previous corruption schemes. See Transparency International – Defence & Security, "Urgent need for full independent inquiry to get to the bottom of who is responsible after two men acquitted of paying bribes in corrupt Saudi arms deal," March 6, 2024, https://ti-defence.org/gpt-corruption-case-uk-saudi-arabia-bribery/ (accessed February 23, 2026); Jasper Jolly, "'There's a bit of a queue forming': how UK firms are enticing buyers for the next generation of fighter jets," *The Guardian*, July 16, 2025, https://www.theguardian.com/uk-news/2025/jul/16/theres-a-bit-of-a-queue-forming-how-uk-firms-are-enticing-buyers-for-the-next-generation-of-fighter-jets (accessed February 23, 2026).

[9] Transparency International – Defence & Security, *GDI 2020 Global Report: Disruption, Democratic Governance, and Corruption Risk in Defence Institutions*, (London: Transparency International UK, 2021), pp. 10-15, https://ti-defence.org/gdi/wp-content/uploads/sites/3/2022/02/GDI-Global-Report-v7_17Feb22.pdf. The GDI is published every five years, therefore the edition used here is the 2020 one, the most recently available; at the time of publication, the results of the 2025 edition were not yet available.

[10] Sabrina White, Yi Kang Choo, Denitsa Zhelyazkova, and Patrick Brobbey, *Sabotaging peace: Corruption as a threat to international peace and security*, (London: Transparency International-Defence & Security, April 2025), pp. 16-20 https://ti-defence.org/wp-content/uploads/2025/06/Corruption-as-a-threat-to-peace-and-security.pdf.

[11] GIZ, *Anti-Corruption in Fragile Settings.*

[12] Institute of Economics and Peace, *Peace and Corruption*, 2015, https://www.economicsandpeace.org/wp-content/uploads/2015/06/Peace-and-Corruption.pdf; GIZ, *Anti-Corruption in Fragile Settings*; Darren Acemoglu and James A. Robinson, *Why Nations Fail. The Origins of Power, Prosperity, and Poverty* (New York: Crown Currency, 2012).

representative of local communities. In Afghanistan in 2005–2021, ever-present government corruption was, as journalist Sarah Chayes put it, 'fodder for an expanding insurgency,' providing not only motivation, but also the resources and a wellspring of civilian support for Taliban groups.[13]

While corruption in any sector can have detrimental impact, corrupt practices in the justice, security and defence sectors appear to be particularly pernicious. A corrupt judiciary and police force have ample opportunities to prey on and humiliate the population, enable corruption elsewhere to flourish, and remove the last recourse individuals have within the state.[14] Defence corruption can have day-to-day impact in countries where the military has a direct role in the life of a country, especially in cases of domestic conflict. One study of motivations that push individuals to join extremist groups suggests that distrust in the defence and security forces proves crucial: 78% of those interviewed had low levels of trust in the police, military and politicians, and 71% reported an arbitrary killing or arrest of a friend or family member as their tipping point.[15]

In addition to contributing to the outbreak of conflict, a lack of attention to widespread corrupt practices can derail attempts at achieving peace settlements, especially in civil wars that contest the control of state structures and resources. Peace agreements usually involve a redistribution of power and access to resources structured to attract the main belligerent groups and render peace a more viable option than continued combat. The security and defence sector has a unique place in these settlements, as it usually integrates former combatants into state structures; participation in turn provides warring groups with a degree of security in the post-war order. This can provide short-term stabilization and an incentive to negotiate, but in the long term, it can become an opportunity for powerful individuals and networks to consolidate their influence, and can result in state capture. Security and defence institutions, with greater secrecy levels and significant budgets, can become channels through which resources are funnelled to narrow elites at the expense of other groups and the population overall. Without a wholesale governance reform, the initial peace agreement thus cannot be turned from a narrow, elite-based bargain into a more inclusive political settlement offering a greater number of people a stake in its outcome.

In South Sudan, for example, a peace settlement that led to its independence from Sudan incorporated former combatants and their competing formations into a new armed force, using income from oil exports – which provided up to 96% of the state's revenue–to pay for what was effectively an unreformed patronage structure through either salaries or illicit diversion. By 2012, one estimate pegged the amount of money stolen from the defence budget at USD 4 billion, and key items such as healthcare and education were often funded by donors. This patronage system was challenged by the 2013 worldwide drop in oil prices; with elites no longer able to act as patrons, competing networks attempted to take control of scarcer resources, precipitating the 2013 civil war that killed about 400,000 people, displaced 2.3 million, and saw widespread atrocities.[16]

Another significant pathway for corruption to impede efforts at peace settlements is by derailing the desired outcomes of international peace support and counter-terrorist operations. Since corrupt practices contribute to

---

[13] Sarah Chayes, *Thieves of State: Why Corruption Threatens Global Security,* (New York: W.W. Norton, 2015); Karolina MacLachlan et al, *The Fifth Column. Understanding the Relationship between Corruption and Conflict*, (London: Transparency International-Defence & Security, 2017), https://ti-defence.org/wp-content/uploads/2017/09/The_Fifth_Column_Web.pdf; Transparency International-Defence & Security, *Mali's Defence Sector: Systemic Corruption Risk Amidst Escalating Violence*, Policy Brief, September 2024, p.2, https://ti-defence.org/wp-content/uploads/2025/01/Malis-defence-sector-Systemic-corruption-risk-amidst-escalating-violence.pdf; Philip Obaji, "A Coup Won't End Mali's Corruption and Insecurity," *Foreign Policy*, August 19, 2020, https://foreignpolicy.com/2020/08/19/a-coup-wont-end-malis-corruption-and-insecurity/ (accessed February 23, 2026).

[14] Sarah Chayes, "Corruption and State Fragility," *Fragility Study Group Policy Brief* no.1, September 2016, https://www.usip.org/sites/default/files/Fragility-Report-Policy-Brief-Corruption-and-State-Fragility.pdf.

[15] United Nations Development Programme (UNDP), *Journey to extremism in Africa*, September 7, 2017, https://www.undp.org/publications/journey-extremism-africa.

[16] Alan Boswell, Nanako Yamanaka, Aditya Sarkar and Alex De Waal, "The security arena in South Sudan: a political marketplace study," (Conflict Research Programme, London School of Economics and Political Science, London, UK, 2019), http://eprints.lse.ac.uk/102894/1/De_Waal_the_security_arena_in_south_sudan_published.pdf; Alex de Waal, "When kleptocracy becomes insolvent: Brute causes of the civil war in South Sudan," *African Affairs* 113, no. 452, July 2014, pp. 347–369, https://doi.org/10.1093/afraf/adu028; The Sentry, *The Nexus of Corruption and Conflict in South Sudan* (2015), https://thesentry.org/wp-content/uploads/2015/07/report_NexusCorruptionConflict_SouthSudan_TheSentry.pdf; Naomi Pendle, *Elite Bargains and Political Deals Project: South Sudan Case Study*, (London: UK Stabilisation Unit, 2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/766051/South_Sudan_case_study.pdf; White et al, *Sabotaging Peace*, pp. 42-48.

violent conflict and violent conflict perpetuates corruption, most international military operations – whether in fragile and (post-)conflict states or in more stable areas – will need to understand and mitigate their impact.[19] Operating in environments where state capture has turned state institutions into means of extracting resources to benefit a narrow elite is challenging, and governments and security forces whose activities have been subverted by widespread corruption are not likely to be reliable partners in providing security.[37] As the cases of Iraq, Afghanistan and Mali have shown, training or providing weapons to corrupt and poorly governed security and defence forces is unlikely to result in better security for the population or more effective partner forces. In Afghanistan, political support for malign powerbrokers and an injection of billions of dollars into the Afghan economy through U.S. military contracting and reconstruction projects strengthened corrupt networks, enabled extortion and abuse of civilian populations, and in the end strengthened the appeal and effectiveness of insurgent groups.[17]

'…[T]he ultimate point of failure for our efforts ... wasn't an insurgency. It was the weight of endemic corruption.'

Ryan Crocker, U.S. Ambassador to Afghanistan, quoted in SIGAR (2016)[18]

The activity of international forces can help limit corrupt practices, but it can also exacerbate them; much depends on the conduct of the intervening force and on its ability to navigate the national political power landscape. In particularly problematic cases, corruption within international operations themselves – from selling fuel, food and weapons on the black market to demanding bribes for local contracts and employment and extorting sexual favours in return for basic assistance – can divert resources, damage mission credibility, create grievances and give a tacit green light to local corrupt networks. UN troops in Bosnia and the DRC, for example, traded black market goods from cigarettes and coffee to fuel, gold, ivory and weapons, turned a blind eye to people smuggling, and were reportedly leaving their posts with suitcases of cash.[19]

Controlling the conduct of the force itself is therefore a key starting point, but its planners and commanders also need to be able to understand the impact of their presence and the resources they bring –from political support and international legitimacy for national power brokers, to access to humanitarian aid and contracting budgets. TI-DS's Government Defence Integrity Index, however, suggests that while many militaries have made attempts to address corruption as an ethical issue for their troops, an appreciation of its strategic significance in operations is weak. 67% of countries assessed showed a critical level of risk in operations, with very few who have addressed corruption in their doctrine, forward planning, or contracting guidance (this is the case in 16 out of 22 NATO member states assessed in the Index). Compounding the problem is a lack of anti-corruption training and weak implementation of codes of conduct among top contributors to UN and, to a lesser extent, NATO missions.[20] Without a concerted effort to understand the impact of corruption in operations, it will continue to undermine future deployments.

Impeding Legitimate Responses to Conflict and Insecurity: Corruption and Gutted Militaries

Corrupt practices significantly influence the armed forces' combat readiness. They waste the resources necessary to procure equipment and weapons, and weaken troop preparedness and morale through a lack of key supplies, irregularities in recruitment and promotions, and payment chains that enable withholding of salaries and the existence of ghost soldiers. Procurement, especially international arms transfers, is one of the areas of the

[17] Chayes, *Thieves of State*; Special Inspector General for Afghanistan Reconstruction*, Corruption in Conflict: Lessons from the U.S. Experience in Afghanistan* (Washington, DC: SIGAR, 2016); Transparency International - Defence & Security, *Afghanistan: Corruption and the making of warlords*, Interventions Anti-Corruption Guidance, (London: Transparency International UK, 2018), https://iacg.ti-defence.org/casestudy/afghanistan-corruption-and-the-making-of-warlords/ (accessed February 23, 2026).
[18] *Corruption in Conflict* (SIGAR), p. i.
[19] Transparency International - Defence & Security*, Corruption and UN peace operations*, Interventions Anti-Corruption Guidance*,* London: Transparency International UK, 2019, https://iacg.ti-defence.org/casestudy/corruption-and-un-peace-operations/ (accessed February 23, 2026).
[20] TI-DS, *GDI 2020 Global Report*, pp. 17-21.

defence and security sector most vulnerable to corruption. Shielded by high levels of secrecy, arms sales can hide bribes by inflating the cost of weapons or delivering sub-standard equipment. According to Transparency International–Defence & Security, about 30% of the countries analysed in the most recent Government Defence Integrity Index- including many major arms importers – make very little procurement-related information available; this includes 55% of top importing countries that are at high to critical risk of corruption.[21] The habits of secrecy shaping limited oversight of defence and security forces make corrupt schemes more difficult to uncover in peacetime and more likely to be revealed by a crisis, with key consequences for both human and state security.

In Nigeria, for example, corruption at all levels of the defence and security forces – from irregularities in recruitment, promotions and salary payments to billions of dollars being stolen from the defence budget through fraudulent procurement deals – has made it difficult for its armed forces to tackle external threats and manage internal issues. Investigations have revealed that in 2000–2020, USD 15 billion was embezzled from the military budget by corrupt officials enabled by a lack of transparency and oversight, while a lack of equipment (including helicopters and ammunition that were never delivered) placed frontline troops in danger. This has left Nigeria's military struggling to counter piracy in the Niger Delta and the Gulf of Guinea, tackle Boko Haram, manage inter-community crises, or stem the flow of illicit weapons into the country. Nigerian units have also been implicated in illegal oil bunkering in the Niger Delta, selling arms to militias, and abuse of the civilian population.[22]

The failure of the Iraqi military against ISIS in 2014 is another illustration of the impact of corruption. The city of Mosul was taken by an ISIL force numbering under 2,000, facing a combined force of the Iraqi army's 2nd Division and the 3rd Division of the police that, on paper, numbered 25,000. In reality, however, that number was closer to 10,000: the ranks were full of ghost soldiers, only existing on paper so that commanders could pocket their salaries. The actual force was unpaid, underfed and under-equipped, as senior officers embezzled funds and sold fuel and troop rations on the black market. The politicization of the armed forces, with potential Sunni opponents removed in favour of Shia loyalists, further degraded military capability and turned the army into a market where high-ranking positions were bought and sold, and where commanders later made up their financial outlay by preying on subordinates. The effect was a force that could not feed or equip its personnel, let alone conduct effective military operations.[23]

Ukraine, which has been defending itself against Russia's attacks – from the fomenting and support of separatist movements in 2014 to the full-scale invasion in 2022 – for over a decade, has made concerted efforts to counter corruption in the armed forces, especially as corrupt practices have often been linked to Russia's efforts to foster Ukrainian dependence.[24] Starved of cash after the collapse of the Soviet Union, the Ukrainian armed forces had been expected to pay for some of their needs through selling off surplus or obsolete equipment and liquidating MoD-owned real estate. With high levels of secrecy and a lack of meaningful oversight, asset disposal transactions came to support corrupt networks at all levels. At higher levels, the ability to conduct procurement and budgeting in secrecy and without competition made it easier to hide bribes through bloated prices. Corruption also flourished in the management of military housing, military education and training, and selection of personnel for international peace support operations.[25] By 2014, Ukraine had a military that was badly

[21] TI-DS, *GDI 2020 Global Report*, p. 11.
[22] Daniel Kofi Banini, "Security sector corruption and military effectiveness: the influence of corruption on countermeasures against Boko Haram in Nigeria," *Small Wars & Insurgencies* 31, no.1 (2020): 131-158, https://doi.org/10.1080/09592318.2020.1672968; Transparency International – Defence & Security, *Nigeria's Defence Sector: Persistent Corruption Risk Among Escalating Security Threats*, Policy Brief, (London: Transparency International UK, July 2024), https://ti-defence.org/wp-content/uploads/2025/01/Nigerias-defence-sector-Persistent-corruption-risk-amidst-escalating-security-threats.pdf; International Crisis Group, Nigeria: The Challenge of Military Reform, Crisis Group Africa Report no. 237 (June 6, 2016), https://www.crisisgroup.org/africa/nigeria/237-nigeria-challenge-military-reform.
[23] Yasir Abbas and Dan Trombly, "Inside the Collapse of the Iraqi Army's 2nd Division," *War on the Rocks*, July 1, 2014, https://warontherocks.com/2014/07/inside-the-collapse-of-the-iraqi-armys-2nd-division/ (accessed February 23, 2026); Ned Parker, Isabel Coles, and Raheem Salman, "How Mosul Fell: A General's Story," *Reuters*, October 14, 2014, http://graphics.thomsonreuters.com/14/10/MIDEAST-CRISIS:GHARAWI.pdf.
[24] Another chapter in this volume analyses the significance of corruption as a tool of hybrid warfare. See also Karolina MacLachlan, *Corruption as Statecraft: Using Corrupt Practices as Foreign Policy Tools*, Transparency International – Defence & Security, July 2019, https://ti-defence.org/wp-content/uploads/2019/11/DSP_CorruptionasStatecraft_251119.pdf.
[25] Leonid Polyakov, "Corruption Obstructs Reforms in the Armed Forces," in *Almanac on security sector governance in Ukraine*, ed. Joseph L. Derdzinski and Valeryia Klimenko, (Geneva and Kyiv: DCAF and the Razumkov Centre, 2012), pp. 81-92.

equipped, underpaid, and unable to provide frontline soldiers with what they needed. Many who were drafted at that time had to secure their own weapons and equipment; volunteers replaced the military logistics chains to deliver equipment to the frontlines; there was crowdfunding for everything from boots to night-vision goggles to drones; and soldiers still reported officers stealing equipment from warehouses.[26] Russia's full-scale invasion created additional pressures on defence governance: the urgency of procuring equipment, supplies and ammunition in a limited and competitive market has led to a greater use of middlemen – including those under investigation for misconduct–and significantly more resources being poured into defence procurement. Since 2022, several high-profile corruption scandals involved both high-level defence officials and companies contracted to make urgent deliveries, and corrupt practices have affected crucial military equipment with a direct bearing on operational effectiveness: drones and ammunition.[27]

Throughout the war, the Ukrainian government has continued to implement significant anti-corruption and governance reforms in the defence sector initiated in 2014. So far, this has included the corporatisation of the state-owned defence conglomerate Ukroboronprom, creation of new procurement offices within the Ministry of Defence, enabling the scrutiny of non-classified defence procurement by civil society, strengthening parliamentary scrutiny, working to bring procurement regulations in line with NATO standards, and creating investigative bodies specializing in investigating and prosecuting corruption, including in the defence sector.[28] Ukrainian society continues to rate corruption as a key domestic issue and civil society continues to exert pressure on the executive, helping to limit the extent and impact of corruption on the country's war effort.[29]

The pernicious effects of corruption are not limited to fragile and conflict-affected states, affecting the world's stronger militaries as well. In the so-called Fat Leonard scandal, senior U.S. naval officers have been charged with accepting bribes, luxury trips and items, and sexual favours from 'Fat Leonard' Glenn Francis, owner of Glenn Defense Marina Asia (GDMA), a contractor providing port services to the 7th Fleet in Southeast Asia, and Australia and the Pacific Islands. In return, officers steered contracts towards GDMA; approved bills that significantly overcharged the Navy; and protected GDMA from detection. The Navy's Criminal Investigative Service (NCIS) estimates that the Navy has lost USD35 million in false invoicing to GDMA over two decades. Corruption has also impacted operational security as officers leaked classified ship schedules to Francis and steered vessels to ports where GDMA was the service provider.[30] This compromised the 7th Fleet's function as a means of signalling intention and projecting power in the Pacific, especially in areas where freedom of navigation was being challenged: with vessel routes and priorities being determined by factors other than strategic considerations, their utility as tools of national security and foreign policy was limited. The scandal has implicated hundreds of

[26] *The Daily Beast*, "Corruption eats away at Ukraine military," *Kyiv Post*, October 23, 2014, https://www.kyivpost.com/content/ukraine-abroad/the-daily-beast-corruption-eats-away-at-ukraine-military-369126.html (accessed February 23, 2026); Chris Dunnett, "How Volunteers Created a 'Second State' Inside Ukraine," *Hromadske International*, January 31, 2015, https://hromadske.ua/en/posts/how_volunteers_created_second_state_inside_ukraine (accessed February 23, 2026); Stewart Philippa H., "Ukraine: A war funded by people's donations," *Al Jazeera,* April 21, 2015, https://www.aljazeera.com/features/2015/4/21/ukraine-a-war-funded-by-peoples-donations (accessed February 23, 2026); Sarah Chayes, "How Corruption Guts Militaries: The Ukraine Case Study," *Defense One*, May 16, 2014, https://www.defenseone.com/ideas/2014/05/how-corruption-guts-militaries-ukraine-case-study/84646/ (accessed February 23, 2026).

[27] Anna Fratsyvir, "Ukrainian lawmaker, ex-governor jailed in drone procurement corruption case," *The Kyiv Independent*, August 4, 2025, https://kyivindependent.com/ukrainian-lawmaker-detained-in-in-drone-procurement-corruption-case/ (accessed February 23, 2026); Kateryna Tyschenko and Valentyna Romanenko, "Embezzlement of $39 million: Defence Ministry officials and Lviv Arsenal managers exposed," *Ukrainska Pravda*, January 27, 2024, https://www.pravda.com.ua/eng/news/2024/01/27/7439191/ (accessed February 23, 2026); White et al, *Sabotaging peace,* pp. 37-40.

[28] White et al, *Sabotaging peace,* pp. 37-40

[29] Mykhailo Minakov, "Ukraine at War Must Deal with the Threat of Strategic Corruption," *Wilson Center*, November 13, 2024, https://www.wilsoncenter.org/blog-post/ukraine-war-must-deal-threat-strategic-corruption (accessed February 23, 2026); Kateryna Ordachenko and Oleksandr Poznii, "Ukrainians see corruption as a key issue during the war," *Wilson Center*, July 31, 2024, https://www.wilsoncenter.org/blog-post/ukrainians-see-corruption-key-issue-even-during-war (accessed February 23, 2026).

[30] Jesse Hyde, "Fat Leonard's Crimes on the High Seas," *Rolling Stone*, March 11, 2018, https://www.rollingstone.com/politics/politics-news/fat-leonards-crimes-on-the-high-seas-197055/ (accessed February 23, 2026); Tom Wright, "Fat Leonard," *Project Brazen podcast*, 2021, https://brazen.fm/podcasts/fat-leonard/ (accessed February 23, 2026).

officers, including admirals, stalling careers and precluding those with Pacific-related operational experience from progressing through the ranks.[31]

'China could never have dreamt up a way to do this much damage to the U.S. Navy's Pacific leadership.'
Senior U.S. Pacific Command Staff member, quoted in LaGrone (2021)

Diverting Weapons, Strengthening Organized Crime

In addition to fostering an environment conducive to conflict and impeding responses to violence, corruption in the defence sector can also deliver the means of warfare by enabling weapons smuggling to organized crime groups, terrorist organizations, and militia. As discussed above, arms transfers and defence procurement are uniquely vulnerable to corrupt practices at all levels, including million-dollar embezzlement from contracts for major weapons systems. Corruption is also a facilitator of arms diversion at lower levels, benefiting armed actors in conflict zones as well as organized crime groups. In a recent analysis of arms diversion pathways, Tl-DS has identified unauthorized sales of arms from national stocks by defence personnel as a key mechanism of arms diversion. The majority of the 400 diversion cases reviewed by TI-DS involved low-level corruption, often motivated by unpaid or low salaries and extortion of bribes in recruitment and promotion chains; however, the involvement of mid- to high-level officials was not uncommon. In more than half of these cases, security forces had diverted weapons to armed militants and organized crime groups, often resulting in deaths, injuries and abuse of civilians.[32]

In Colombia, for example, defence units working with narco-traffickers and paramilitary groups – often as much due to resource shortages and a lack of systemic support as for monetary gain – protected gang territory, helped secure access for contraband, and smuggled out the finished product. Serving and retired personnel have been investigated for selling over 2,000 grenades and 150,000 rounds of ammunition to a militant group.[33] In Kenya, police personnel – motivated primarily by low or unpaid salaries – sold rifles and ammunition to armed groups and militias, exacerbating inter-community tensions.[34] A similar pattern emerged in Afghanistan: weapons and equipment supplied by the U.S. to the Afghan National Army and Police ended up in the hands of the Taliban due to a mixture of battlefield capture, weak stockpile management, and corruption, with soldiers and officers selling their US-provided weapons to the adversary.[35] In Mali, widespread collusion between security and defence forces and organized crime helped make the country the 'epicentre' of arms and drug trafficking, challenging state authority and leading to increasing abuse of the civilian population.[36] And in Nigeria, guns and ammunition missing from the army's Central Ordnance Depot were tracked to insurgent groups in the Niger Delta that the armed forces were tasked to control.[37]

Weak stockpile security and lax export control and verification measures facilitate corruption-mediated diversion. Gaps in recordkeeping and physical condition and monitoring of storage facilities contributed to diversion in over half of cases reviewed by TI.[38] In international arms trade, corruption and lack of transparency prevent meaningful control over the final destination of weapons. US weapons exported to Saudi Arabia and the UAE, for example, have ended up in the hands of militia in Yemen; in the Sahel region, Amnesty International has

[31] Sam LaGrone, "Lawmakers Survey: 94% of Sailors Say 'Damaging Operational Failures' Related to Navy Culture, Leadership Problems," *USNI News*, July 12, 2021, https://news.usni.org/2021/07/12/lawmakers-survey-94-of-sailors-say-damaging-operational-failures-related-to-navy-culture-leadership-problems (accessed February 23, 2026).
[32] Michael Picard and Colby Goodman, *Under the Radar: Corruption's Role in Fueling Arms Diversion*, Transparency International US and Transparency International-Defence & Security, April 2025, p.6, https://ti-defence.org/wp-content/uploads/2025/04/Under-the-Radar-Corruptions-Role-in-Fueling-Arms-Diversion.pdf.
[33] Hannah Stone, *Corruption and Plan Colombia: The Missing Link* (London: Transparency International Defence & Security, 2019), https://ti-defence.org/wp-content/uploads/2020/01/0619_DSP_Colombia_WEB.pdf; Picard and Goodman, *Under the radar*, p. 19.
[34] Picard and Goodman, *Under the Radar*, pp. 20-22.
[35] Austin Bodetti, "How the US Is Indirectly Arming the Taliban," *The Diplomat*, June 13, 2018, https://thediplomat.com/2018/06/how-the-us-is-indirectly-arming-the-taliban/ (accessed February 23, 2026).
[36] Transparency International-Defence & Security, *Mali's Defence Sector*, p. 4.
[37] International Crisis Group, *Nigeria: the Challenge of Military Reform*, p. 13.
[38] Picard and Goodman, *Under the Radar*, p. 36.

tracked weapons used by armed militias to a number of European exporters, including Serbia, France, the Czechia and Slovakia.[39] Most recently, illicit weapons have been found in Sudan in violation of the UN embargo, fuelling one of the most cruel and deadly conflicts of the 2020s. In all cases, corruption and trafficking are likely to have played a significant role in enabling sanctioned armed groups to capture weapons and prolong deadly conflicts.[40]

Conclusion

Corruption in the defence and security sector has a multi-faceted impact on peace and security: from misdirecting resources that could be spent on development to waste impacting military readiness to exacerbating or creating grievances, failing to respond to specific threats, and undermining international efforts to bring peace. Corruption and conflict are often enmeshed in a vicious cycle: while corrupt practices contribute to violent conflict, violent conflict itself can exacerbate the reach and depth of corruption by creating new pressures on institutions and depleting resilience. Corruption can also make the recurrence of conflict more likely as it undermines peace agreements, derails international peace support interventions, and facilitates arms diversion, thus helping equip terrorist organizations, militias, and organized crime groups.

These effects are all exacerbated when corruption affects the defence and security sector, with its resources, secrecy and centralization offering extra opportunities for corrupt schemes. But despite the impact of corruption, many military and civilian actors in the security realm treat it as a secondary problem that takes a back seat to war-fighting considerations. This leads to neglecting key factors shaping not only development and state and societal resilience, but also operational preparedness and the ability of international organizations to deliver on their goals. Left unchecked, corruption can determine the success or failure of an operation and the success or failure of a whole defence force. In the current environment, where insecurity is on the rise and so are defence budgets, governments and defence institutions cannot afford to ignore the risks that corruption poses. They would be risking not only the loss of resources, but also lower preparedness and broken trust between armed forces and societies whose involvement is needed for effective military operations.

[39] CNN, "Yemen: Lost U.S. arms," February 2019, https://edition.cnn.com/interactive/2019/02/middleeast/yemen-lost-us-arms/ (accessed February 23, 2026); Amnesty International, "Sahel: Amnesty identifies Serbian weapons in stockpiles of brutal armed groups," August 24, 2021, https://www.amnesty.org/en/latest/news/2021/08/sahel-amnesty-identifies-serbian-weapons-in-stockpiles-of-brutal-armed-groups/ (accessed February 23, 2026).
[40] White et al, *Sabotaging Peace,* p. 36.

2. Corruption as a Weapon in the Modern Hybrid-Influence Toolbox

Alexandra Addison-Wrage[1]

The 1990s opened with two global events that prompted a profound and ongoing re-evaluation by the West's adversaries of military strategy. In the first Gulf War, the lopsided superiority of the U.S.–led multinational forces and their high-tech long-range precision weapons was striking. Technological superiority mattered more than numerical advantage.[2] That same year, the collapse of the USSR'–seen by Vladimir Putin as 'the greatest geopolitical catastrophe' of the last century – made plain the consequences of Soviet leadership allowing itself to be goaded into competing with the United States and NATO in a costly, high-tech missile and nuclear-arms race.[3] With nuclear overcapacity and no realistic way to match Western technological advances, Russian and Chinese military thinkers concluded they had to punch above their weight–without provoking a superior military response. They accordingly undertook a project of redefining war itself, including seeking 'new concepts of weapons' for pursuing such wars.

Many of the ideas behind the re-envisioned Russian 'new generation warfare' and Chinese 'unrestricted' or 'beyond-limits warfare' were actually neither new nor entirely homegrown. What was new, however, was the abandonment of traditional rules, distinctions and taboos; the blurring of lines between wartime and peacetime, and between the domains of armed forces and intelligence services; the borrowing of and expansion of techniques of espionage such as the 'active measures' employed by the KGB. There was also experimentation with and testing of such methods, domestically and in the 'near abroad' and in proxy conflicts, with the intent of deploying them widely on a globalized battlefield against the West, rather than relying on the limited, plausibly deniable deployment of the past. This chapter will address how corruption has been developed and exploited as a tool of hybrid influence.

The Past and Present of Hybrid Influence

This section examines how such practices can be deliberately exploited and instrumentalized by state actors. Rather than viewing corruption solely as a governance failure, the following analysis explores its potential use as a strategic tool by Russia and China to exert influence, undermine institutions, and advance geopolitical objectives. The weaponisation of corruption is examined not as a means of private enrichment, but as a tool for pursuing public and strategic objectives that benefit a state or a group of states.

Russia

In a widely cited article from 2013 entitled 'The Value of Science Is in the Foresight', the Chief of the General Staff of the Russian Armed Forces, General Valery Gerasimov, called attention to a recent evolution in the nature of war:[4]

---

[1] Alexandra Addison-Wrage is the President of TRACE: https://www.traceinternational.org/

[2] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, trans. Foreign Broadcast Information Service (Beijing: PLA Literature and Arts Publishing, 1999), https://www.c4i.org/unrestricted.pdf; S. G. Chekinov and S. A. Bogdanov, "On the Nature and Content of Wars of a New Generation," *Military Thought*, No. 10, (2013): 12–23, https://www.usni.org/sites/default/files/inline-files/Chekinov-Bogdanov%20Miltary%20Thought%202013.pdf; Vladimir Slipchenko, *War of the Future* (Moscow: Moscow Nongovernmental Science Foundation, 1999); Makhmut Gareev, "Nature of Future Wars," *Law and Security* 1-2 (June 2003) available (in Russian) at http://dpr.ru/pravo/pravo_5_4.html.

[3] Liang and Xiangsui, *Unrestricted Warfare*, p. 23; Yeliseeva Natalya Viktornovna, "Collapse of the Communist Regime: Bankruptcy and Disintegration of the USSR," *Perestroika and Collapse of the USSR*, (Moscow, 2011), available (in Russian) at http://www.ru-90.ru/node/501; Nikolay Nelyubin, "Nuclear Arsenals are Still Redundant," *Novyy Prospekt*, July 30, 2021, available (in Russian) at https://newprospect.ru/news/interview/yadernye-arsenaly-izbytochny-do-sikh-por-perevodchik-gorbachyeva-pro-znachenie-dogovora-snv-spustya-/.

[4] Valery Gerasimov, "The Value of Science Is in the Foresight," *Military-Industrial Kurier*, February 27, 2013, (in Russian, as translated into English by the author). Many of Gerasimov's points were anticipated by Gareev in 2003 and Chekinov and Bogdanov in 2010–2013. See

> In the 21st century there has been a discernible tendency to blur the lines between the states of war and peace. Wars are no longer declared, and having begun, they proceed according to a pattern to which we are not accustomed. […]
>
> The 'rules of war' themselves have changed. The role of nonmilitary methods has grown in achieving political and strategic goals, and, in a number of cases, they have exceeded the power of force of weapons in their effectiveness. The focus of confrontation methods that are employed has been shifting toward the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—carried out with the help of the protest potential of the population. […]
>
> Asymmetrical actions have become widespread, allowing one to neutralize an enemy's superiority in armed conflict. Among these are the use of special operations forces and internal opposition to create a permanently operating front throughout the entire territory of the enemy state, as well as information influence whose forms and means are being constantly perfected.

According to Gerasimov, this strategic shift away from direct military engagement and toward the deployment of 'political, economic, informational, humanitarian, and other nonmilitary measures' required the Russian military to reevaluate its own approach to war. The country should pursue a systematic, scientific evaluation of the new operational environment and prepare an appropriately prescient response.

The development of such a response would be influenced by the character of Russia's post-millennial leadership.[5] For the first time in the country's history (with one minor exception),[6] the country's highest office was held, then retained for more than two decades, by a Chekist: a loyal KGB/FSB officer. During Soviet times, the KGB had unlimited resources and significant power, yet it had always been under the control of the Communist Party, and its influence and appetites were checked by the Soviet military establishment. In contrast, Vladimir Putin has reshaped Russia into a Chekist-run state, unshackled from ideological constraints and unchallenged by other power centres, declawing the Russian military leadership *vis-à-vis* the ruling Chekist elites, and adopting KGB/FSB methods and tactics wholesale.

Those methods and tactics encompass much of what the West learned during the Cold War, but has since largely forgotten about Russian espionage techniques: active measures[7] (now renamed 'support' or 'facilitation' measures[8]); reflexive control;[9] agents of influence; *kompromat*, false-flag and monetary-based agent recruitment methods; compromise/discreditation;[10] subversive activity; and 'active reserve' officers (now called 'seconded

---

Timothy Thomas, *The Chekinov-Bogdanov Commentaries of 2010-2017: What did they Teach us about Russia's New Way of War?* (MacLean, VA: MITRE, 2020).

[5] There is a noticeable progression of Russian military thought on new generation warfare from Slipchenko's book in 1999 (before Putin came to power) to Gareev's 2003 article (after Putin's accession) to Chekinov and Bogdanov's writings in 2010 - 2017 and Gerasimov's article in 2013. See Peter Mattsson, "Russian Military Thinking – A New Generation of Warfare," *Journal of Baltic Security* 1, no. 1, (2015): 61-70, https://journalonbalticsecurity.com/journal/JOBS/article/107.

[6] Although Yuri Andropov became the Soviet leader in 1982 after being in charge of the KGB for 15 years, he fell seriously ill and died about a year later before he was able to implement any of his rumoured extensive plans for reshaping the Soviet state.

[7] These were defined by the KGB as 'Agent-operational measures directed at exerting influence on the foreign policy and the internal political situation of target countries in the interests of the Soviet Union …, weakening the political, military, economic and ideological positions of capitalism, undermining its aggressive plans, in order to create conditions favorable to the successful implementation of the Soviet Union's foreign policy, and ensuring peace and social progress.' These and some other KGB terms can be found in Vasili Mitrokhin (ed.), *KGB Lexicon: The Soviet Intelligence Officers Handbook* (London: Frank Cass, 2002).

[8] According to a 2015 textbook for Russian operations officers, which was publicly available online for a short time, one of the two main objectives of Russia's security services involves 'support measures to exert intelligence influence on government circles of foreign countries with the aim of inducing them to make decisions of the political, military-strategical or economic nature that are beneficial to our country.'

[9] 'Reflexive control is the practice and theory of controlling one's opponent by causing them to act as a 'reflex' to disinformation or deception. When using reflexive control, one conveys specially designed information, or disinformation, to provoke a reaction leading the opponent to voluntarily make the predetermined decision the initiator desires.' Natalie Minton, "Cognitive Biases and Reflexive Control," (University of Mississippi, 2017).

[10] 'Compromise/discreditation is a method for Intelligence to inflict moral and political harm on an adversary, to undermine the authority and weaken the positions of its state institutions, political organizations and individual persons by publicizing specially selected materials and information, whether real or fabricated, about unconstitutional or amoral acts, which have been committed by them and which are

officers'). These concepts are no longer the sole domain of the Russian 'soldiers of the invisible front,' and their use is no longer limited to covert actions such as were once occasionally authorized but tightly controlled by the Politburo. Rather, they are being put into service as part of a "new concept of weapon" in the reimagined new generation warfare against the West.

We need to recognize the expanded scope of this new form of warfare: it is no longer confined to military confrontation, but extends across the full range of inter-state relations. Marius Laurinavičius argues that 'the Clausewitzian concept of total war describes Russia's strategy against the West much more accurately than hybrid warfare, non-linear war, or even new generation warfare' because 'total war makes no distinction between war and peace, while hybrid warfare and non-linear war refer to several non-military forms of warfare undertaken in preparation for a conventional war or as a complement to traditional military activity.'[11]

In this ongoing war, Russia has weaponized energy, information and refugee crises. Corruption, too, can be considered an element of this expanded toolkit. Laurinavičius believes that 'we should now begin to treat corruption as another weapon in Russia's anti-Western arsenal.'[12] Indeed, in 2018, before becoming President of the United States, Joe Biden acknowledged that 'Russia has managed to effectively export the corruption that has warped its own politics and economy– weaponizing it, in a sense, and aiming it at vulnerable societies elsewhere' and that corruption is such an effective weapon because of 'the difficulty of proving that it even exists, or that its purpose is political.'[13]

It has since become obvious that core Western countries are in no way immune to this particular weapon, and that they may have already been under this kind of attack for years. Examples include lucrative appointments of former German and Austrian politicians and senior government officials to the boards of Gazprom's Nord Stream 2 and Rosneft;[14] and the alleged funding of European far-right parties.[15]

In 2012 and 2013, Russian military strategists were already publicly describing bribery of government and military officials–along with intimidation, deception, blackmail, mass-scale propaganda and other measures–as a tactical resource in new generation warfare. Their aim was to cause–or amplify– chaos before conflict even begins and in the initial period of war. A major objective of weaponized bribery is to force officials of the target country 'to abandon fulfilment of their service duties and, in this way, to manipulate their behaviour' in order 'to create a favorable military, political, and economic setting for the operations of the [aggressor state's] armed forces.'[16]

As an extensive example of the use of corruption and bribery in furtherance of overtly military objectives, we can look at Russia's activities before and during its operations in Ukraine. As revealed in numerous contemporaneous and retrospective reports, Russian 'little green men,' agents and other hybrid warriors extensively used bribery and other measures in 2014 during the annexation of the Crimea, war in Donbas and

---

criminally punishable under the laws of the particular country or condemned by public opinion.' *Common Dictionary of the Chekist Terminology*, edited by F.D. Bobkov, (Higher School of KGB, 1988) (in Russian, based on the excerpts quoted in publicly available works).

[11] Marius Laurinavičius, *Weaponizing Kleptocracy: Putin's Hybrid Warfare* (Hudson Institute, June 2017): p. 10.

[12] Laurinavičius, *Weaponizing Kleptocracy*, p. 13. Other Western observers have also noted the trend toward weaponization of corruption. See, e.g. Multinational Capability Development Campaign, *A Deadlier Peril: The Role of Corruption in Hybrid Warfare*, March 2019; Karolina MacLachlan, *Corruption as Statecraft: Using Corrupt Practices as Foreign Policy Tools* (Transparency International, 2019); Commission on Security and Co-operation in Europe, "Threat of Foreign Corruption to be Explored at Helsinki Commission Hearing," November 12, 2021, https://www.csce.gov/press-releases/threat-foreign-corruption-be-explored-helsinki/ (accessed February 23, 2026).

[13] Joseph R. Biden, Jr. and Michael Carpenter, "How to Stand Up to the Kremlin," *Foreign Affairs,* December 5, 2017, https://www.foreignaffairs.com/articles/russia-fsu/2017-12-05/how-stand-kremlin (accessed February 23, 2026).

[14] Claudia von Salzen, "Nord Stream 2: Neuer Job für Gerhard Schröder bei Gazprom-Tochter," *Tagesspiegel*, October 5, 2016, https://www.tagesspiegel.de/politik/neuer-job-fur-gerhard-schroder-bei-gazprom-tochter-4901833.html (accessed February 23, 2026); "Austrian Ex-Foreign Minister Who Danced With Putin Gets Rosneft Board Seat," *Moscow Times,* June 2, 2021, https://www.themoscowtimes.com/2021/06/02/austrian-ex-foreign-minister-who-danced-with-putin-gets-rosneft-board-seat-a74082 (accessed February 23, 2026).

[15] Kylie Atwood, Michael Conte and Devan Cole, "Russia has spent over $300 million on influencing foreign elections since 2014, US officials say,: *CNN*, September 13, 2022, https://edition.cnn.com/2022/09/13/politics/russia-foreign-elections-influence/index.html (accessed February 23, 2026).

[16] Chekinov and Bogdanov, "The Nature and Content of a New Generation War," p. 19. Similarly, although bribery was not specifically mentioned, Gen. Gareev saw, as one of three main defence priorities for the Russian state in 2003, to 'create favorable external political conditions for the use of armed forces and other troops,' 'securing allies and support of local population in a conflict zone.'

other actions against Ukraine. Specifically, through intimidation, bribes and promises of future rewards, they were able to convince Ukrainian government officials, military, security and law enforcement officers to refrain from resisting, disarm, surrender and switch sides *en masse* in Crimea and many central and eastern Ukrainian regions.

According to the TRACE report, a number of senior officials from the Yanukovich administration had already been compromised by their involvement in grand corruption and the illegal and violent suppression of public protests, and fled to Russia, leaving Ukraine in disarray.[17] Russian agents cajoled, bribed and intimidated members of Ukrainian regional legislatures in an effort to coerce them to proclaim 'independent' people's republics.

When that failed in all but two regions (three if one includes Crimea), Russian agents and proxies called for splitting Ukraine up through federalization. Average Ukrainians were recruited to appear at pro-Russian street protests as 'rented audiences' to simulate popular support calling for Russian invasion and the dismemberment of Ukraine under the slogan, 'Putin, send the troops!' Phone intercepts and email leaks, especially those from Kremlin senior advisors Sergey Glazyev and Vladislav Surkov, later revealed accounting reports for money spent—and for repeated demands by on-the-ground Russian agents for more funding from the Kremlin for these actions.[18]

One of the most striking examples of an official corrupted by Russia is Rear Admiral Denis Berezovskiy. He had a meteoric career in the Ukrainian Navy, receiving the command of the flagship Hetman Sahaydachniy at 28, and then being promoted to Captain 1st rank at 35 and Rear Admiral at 38. He supervised, together with U.S. Navy Capt. James Aiken, the U.S.-Ukrainian naval exercises Sea Breeze in 2012 and 2013. On 1 March 2014, when the Russian annexation of the Crimea was well underway, Berezovskiy was appointed Commander in Chief of the Ukrainian Navy.

Upon receiving command, he immediately severed the encrypted communication lines between the Navy's headquarters in Sevastopol and the political leadership in Kyiv. He issued an order for Ukrainian officers, sailors and marines to not resist any attacks and to disarm, handing over weapons, equipment and military installations to the attackers. On 2 March, he was relieved of his command for issuing an unlawful order. On the same day, he appeared on television taking an oath of loyalty to the Kremlin's puppet government in Crimea and was immediately put in charge of the 'Crimean Navy' at the same rank. On 3 March, with support from Russian irregulars, Berezovskiy unsuccessfully attempted to arrest his replacement, Rear Admiral Serhiy Hayduk, and to entice other Ukrainian officers at the Naval headquarters to switch sides. On 24 March, Berezovskiy was appointed Deputy Commander of the Russian Black Sea Fleet; in November 2018, he was appointed Deputy Commander of the Russian Pacific Fleet; and in February 2020, he was promoted to Vice Admiral of the Russian

---

[17] A detailed account of how Ukrainian political elites were subverted by the Kremlin's dark money can be found at Taras Kuzio, *Bribery and National Security: Lessons from Ukraine*, *TRACE* (2019), https://f.hubspotusercontent20.net/hubfs/5002429/Promotional%20Materials/Publications/White%20Papers/2019%20Bribery%20and%20National%20Security%20Lessons%20from%20Ukraine.pdf. Also see Stephen Grey, Tom Bergin, Sevgil Musaieva, and Roman Anin, "Putin's Allies Channelled Billions to Ukraine Oligarch," *Reuters,* November 26, 2014, https://www.reuters.com/article/markets/special-report-putins-allies-channelled-billions-to-ukraine-oligarch-idUSL3N0TF4QD/; Svyatoslav Khomenko, "Команда Януковича від А до Я: одні ще тут, інші далеко," *BBC News*, February 20, 2015, https://www.bbc.com/ukrainian/politics/2015/02/150220_yanukovych_team_sx; Yana Polyanska, "Захоплення Криму готувалось із 2010 року: нові свідчення у справі Януковича," *Radio Svoboda*, February 7, 2018, https://www.radiosvoboda.org/a/29025846.html; Sergey Mokrushin, "Заочный арест Павла Лебедева: удастся ли Украине достать бывшего министра обороны в аннексированном Крыму?," *Krym.Realii*, May 29, 2020, https://ru.krymr.com/a/zaochnyi-arest-pavla-lebedeva-udastsa-li-ukraine-dostat-ego-v-krymu/30641246.html (all sources accessed February 23, 2026).

[18] See, for example, Shandra and Seely, *Surkov Leaks*; Olena Makarenko and Alya Shandra, "Ukraine Publishes Video Proving Kremlin Directed Separatism in Eastern Ukraine and Crimea," *Euromaidan Press,* August 23, 2016, http://euromaidanpress.com/2016/08/23/ukraine-publishes-video-proving-kremlin-directed-separatism-in-ukraine/; Alya Shandra, "Glazyev Tapes, Continued: New Details of Russian Occupation of Crimea and Attempts to Dismember Ukraine," *Euromaidan Press,* May 16, 2019 http://euromaidanpress.com/2019/05/16/glazyev-tapes-continued-ukraine-presents-new-details-of-russian-takeover-of-crimea-and-financing-of-separatism/; Iryna Romaliyska, "Хроніка захоплення Криму. Прослуховування радника Путіна. Частина 1,"*Цензор.НЕТ*, December 21, 2017, https://censor.net/ua/resonance/3040699/hronika_zahoplennya_krymu_prosluhovuvannya_radnyka_putina_chastyna_1; Iryna Romaliyska, "'Януковича народ, бл#дь, вы#бет в этом Севастополе!' Прослушка советника Путина. Часть 2," *Цензор.НЕТ*, December 28, 2017, https://censor.net/ru/resonance/3041683/yanukovicha_narod_bld_vybet_v_etom_sevastopole_proslushka_sovetnika_putina_chast_2 (all sources accessed February 23, 2026).

Navy.[19] Berezovskiy's exact motivations in betraying Ukraine were never uncovered. There are, though, reports from some Ukrainian military experts that Berezovskiy's family had been threatened, and that he had been promised a senior position in the Russian Navy while keeping his rank. The same experts noted that at the time, compensation in the Russian Navy was reportedly at least three times greater than in the Ukrainian Navy.[20]

The events of 2014 demonstrate how Russian military strategists were able to use corruption to carry out their vision of warfare: bribing and intimidating enemy officials into abandoning their duty, and using the protest potential of the population and internal opposition to create a permanently operating front through the territory. Their goal: to sow chaos and prepare a favourable military, political and economic setting for the operations of the armed forces. It is not a surprise that Russians like to quote the saying by Alexander the Great's father, Philip II of Macedon: 'A donkey laden with gold will capture any castle'–so much so that some believe it to be a Russian proverb.[21] Russia has consistently used corruption as a tool to influence Ukraine's political landscape, both prior to and following the launch of its full-scale invasion. Before 2022, corrupt networks, illicit financing, and compromised elites were leveraged to shape decision-making, weaken state institutions, and constrain Ukraine's Euro-Atlantic aspirations. Since the start of the full-scale war, these practices have evolved and intensified, with corruption narratives and selective exposure of alleged wrongdoing being instrumentalized to undermine international support for Ukraine, erode trust among partners, and question the effectiveness of Ukrainian governance.

Box 2.1. Russia Continues to Use Corruption to Influence Ukraine's Politics, Undermining International Support

[Author: Vassil Genchev]

In weaponizing corruption, Russia has relied on proxies inside Ukraine, typically linked to the deposed former pro-Russian president Viktor Yanukovich. This has often been a marriage of convenience, with corrupt politicians prioritizing their own interests and survival above all else. This dynamic is illustrated by the 2020 motion to close the public register of electronic asset declarations for officials, launched by 48 Ukrainian Members of Parliament affiliated with the now-banned pro-Russian Opposition Platform-For Life party. The motion was approved by the Constitutional Court, which also struck down criminal liability for false asset declarations and issued a raft of other rulings that curtailed the powers of anti-corruption bodies. The motion led to street protests and criticism from the European Union, leading to its eventual reversal. 'This decision obviously plays in favour of Russian interests. It deprives of the support of the West that we particularly need and puts under threat all the financial assistance that we were supposed to be received from the IMF and EU,' activist Iryna Shyba was quoted by Ukrainian TV as saying at the time.[22]

President Volodymyr Zelenskyy tabled a draft law on terminating the powers of all Constitutional Court judges following the controversial ruling. While many Ukrainians applauded the President's accession for protecting accountability and anti-corruption measures, in support of his country's European path, others criticized his actions as unconstitutional. Thus, while a key corruption prevention measure was eventually preserved, and

[19] Institute for the Study of War, "Russian General Officer Guide – May 11, 2022," May 11, 2022, https://understandingwar.org/research/russia-ukraine/russian-general-officer-guide-may-11/ (accessed February 23, 2026).
[20] Stepan Gutnik, "'At gunpoint': Berezovsky was forced to betray Ukraine by taking his family hostage," *Censor.net*, March 2, 2014, https://censor.net/ru/news/273791/pod_dulom_avtomata_berezovskogo_zastavili_predat_ukrainu_vzyav_v_zalojniki_ego_semyu (accessed February 23, 2026); Simon Shuster, "Ukraine Troops in Crimea Face Dilemma: To Defect, Flee or Fight," *Time*, March 9, 2014, https://time.com/17356/ukraine-troops-in-crimea-face-dilemma-to-defect-flee-or-fight/, (accessed February 23, 2026).
[21] The saying attributed to Philip II and the stories of him using bribery to conquer Greek cities are based on Diodorus Siculus, The Library of History (Chicago: Loeb Classical Library, 1952) at 16.53 - 16.54, https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Diodorus_Siculus/. Plutarch, The Life of Aemilius (Chicago: Loeb Classical Library, 1918) at 12:10, https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Plutarch/Lives/Aemilius*.html; and other writings.
[22] *BBC Monitoring*, "Ukraine activists protest against court ruling," Report on *One Plus One TV* (Kyiv) broadcast October 30, 2020, https://monitoring.bbc.co.uk/product/c2024xli., (accessed February 23, 2026).

Ukraine continued to fulfil its agreements with the EU and the IMF, the crisis provoked the political and societal divides that Russian hybrid activities typically seek to exploit in Ukraine and elsewhere.

The Russian propaganda machine was quick to amplify divisions and to seek to undermine Ukraine's international standing during another political crisis that took place in the summer of 2025. Anti-corruption activists protested against legislative amendments that limited the independence of the National Anti-Corruption Bureau of Ukraine (NABU) and the Specialized Anti-Corruption Prosecutor's Office (SAPO). Russian state-controlled television and social media accounts supportive of the aggression against Ukraine seized on the protests, providing ample coverage and claiming that the Ukrainian government's position had been weakened due to corruption and poor governance.[23] Claims were aired that Ukraine was embezzling Western assistance. There were reports that Russia's attempt to exploit the protests had gone beyond propaganda–at one of the street rallies, peaceful student demonstrators distanced themselves from a group of masked men burning an effigy of President Zelenskyy. Ukrainian media described the incident as a provocation possibly staged by Russia.[24]

Ultimately, President Zelenskyy swiftly signed a law restoring the independence of anti-corruption bodies, thanking Parliament for 'hearing' Ukrainian citizens. Nonetheless, during the governance-linked political crises of 2025 and 2020, Russian hybrid influence tools either played a major role, or seized the opportunity to sow divisions and undermine international solidarity, in line with their definition from General Valery Gerasimov's article discussed at the beginning of this chapter.

Box 2.2. Russia Uses Corrupt Networks to Sway Elections in Moldova

[Author: Vassil Genchev]

Ahead of Moldova's parliamentary elections in September 2025, a BBC investigation uncovered an underground Russian-funded network seeking to undermine the country's pro-EU governing party.[25] The BBC found links between the secret network and Moldovan oligarch Ilan Shor - sanctioned by the U.S. for 'the Kremlin's malign influence operations' and now a fugitive in Moscow. The network arranged for a fake election poll and trained and recruited individuals, promising to pay them a monthly fee to produce pro-Russian TikTok and Facebook posts ahead of elections. Analysis by the U.S-based Digital Forensic Research Lab (DFRLab) found that the broader network had amassed more than 55 million views and over 2.2 million likes on TikTok from January to September 2025. Moldovan police were quoted as saying that while Shor had focused on directly bribing voters to vote against EU membership at a 2024 referendum, his approach in 2025 had relied on disinformation. Additional reporting by Bloomberg, based on internal Kremlin documents, revealed additional tactics used to influence the elections, including recruiting Moldovans living abroad to vote for pro-Russian parties, and deploying others to stage disruptive protests. Another tactic, described in more detail earlier in this chapter, was the use of compromising material to pressure public officials to disrupt the electoral process.[26] While Moldovan law enforcement managed to disrupt alleged Russian attempts at election interference, conducting operations in the week before the elections, the reported activities illustrate how the Kremlin has been able to tap into pre-existing corrupt networks established by local proxies to further its agenda in the country.

[23] *BBC Monitoring*, "Briefing: Russian TV amplifies protests over Kyiv law on anti-corruption bodies," July 23, 2025, https://monitoring.bbc.co.uk/product/b0004aia, (accessed February 23, 2026).
[24] *BBC Monitoring*, "Briefing: Ukrainian media report Russian 'provocations' at anti-graft protests," July 28, 2025, https://monitoring.bbc.co.uk/product/b0004bmk. (accessed February 23, 2026).
[25] *BBC News*, "How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation", September 21, 2025. https://www.bbc.co.uk/news/articles/c4g5kl0n5d2o (accessed February 23, 2026).
[26] *Bloomberg*, "Revealed: Putin's Secret Plan to Hack Moldova's Pivotal Election," September 22, 2025. https://www.bloomberg.com/news/articles/2025-09-22/moldova-elections-russia-s-plan-to-hack-the-vote (accessed February 23, 2026).

Russia has used corrupt networks to interfere in elections in Moldova by financing political proxies, facilitating vote-buying, and manipulating local power brokers. These practices are intended to distort democratic competition, undermine pro-European forces, and weaken public trust, making corruption a key instrument of Russia's hybrid influence.

Russia employs similar tactics in the Sahel, where it leverages corrupt networks to gain political influence, undermine democratic processes, and entrench its presence.

Box 2.3. Russia's Hybrid Influence in the Sahel

[Author: Vlasta Kovbasa]

Security crises, leaders' lack of integrity, and accusations of corruption have created a fertile ground for a series of military coups in the Sahel region.[27] Russia, as part of its broader hybrid strategy of influence, has leveraged these circumstances to increase its presence there. Moscow has deployed mercenaries–initially through the Wagner Group, and, after the death of Yevgeny Prigozhin in August 2023, via the Kremlin-controlled Africa Corps–while exploiting local discontent with former colonial powers.[28] At the centre of its strategy are resource-for-security bargains, which embed patronage and corruption into governance, allowing Russia to strengthen its durable political influence. As one report notes, a combination of 'lootability'[29] and a weak political system poisoned by rampant corruption creates highly favourable entry conditions for Russian private military companies, and Russia uses various hybrid tools to prime states to such conditions.[30]

CAR. In 2018, the Wagner Group embedded itself in the Central African Republic by providing support to President Touadera in the country's civil war, then in its fifth year. Leveraging a hybridized model of security support, Kremlin-linked actors gained access to the CAR's lucrative resources, annually extracting hundreds of millions of dollars' worth of gold, timber, and diamonds.[31] A 2023 Sentry report notes that 'Wagner has perfected a blueprint for state capture:[32] supporting a criminalized state hijacked by the Central African president and his inner circle, amassing military power, securing access to and plundering precious minerals, and subduing the population with terror.'[33] Corruption facilitated this model: Western funds directed at disarming the rebels and putting an end to the country's violence have for the most part been embezzled.[34]

[27] Daniel Baltoi, "A Deeper Look into the West African Coup Wave," *Foreign Policy Research Institute*, January 9, 2023, https://www.fpri.org/article/2023/01/a-deeper-look-into-the-west-african-coup-wave/ (accessed February 23, 2026).
[28] Niko Vorobyov, "Wagner vs Africa Corps: The Future of Russian Paramilitaries in Mali," *Al Jazeera*, June 16, 2025, https://www.aljazeera.com/news/2025/6/16/wagner-vs-africa-corps-the-future-of-russian-paramilitaries-in-mali (accessed February 23, 2026).
[29] 'Lootability' is a political economy term, referring to countries "with high-value commodities and low or few barriers to market entry." From Linda Bishai, Stephanie Burchard, and Sarah Day, "Russia's Selling, but Who's Buying? Analyzing the Characteristics of PMC Clients in Africa," *Small Wars Journal*, November 14, 2024, https://smallwarsjournal.com/2024/11/14/russias-state-linked-private-military-companies-in-africa/.
[30] Bishai, Burchard, and Day, "Russia's Selling, but Who's Buying?"
[31] Purity Mwambia, "False: With Russia's Support, CAR Significantly Succeeded in Combating Militants," *Voice of America*, March 4, 2025, https://www.voanews.com/a/false-with-russia-s-support-car-significantly-succeeded-in-combating-militants-/7997777.html (accessed February 23, 2026).
[32] State capture is a type of systemic political corruption in which private interests significantly influence a state's decision-making processes to their own advantage.
[33] The Sentry, "Architects of Terror: The Wagner Group's Blueprint for State Capture in the Central African Republic," June 2023, https://thesentry.org/reports/architects-of-terror/; Jean-Fernand Koena, Maja Zivanovic, and Mike Eckel, "Wagner's Successors Wage Campaign of Terror in Central African Republic," *Radio Free Europe/ Radio Liberty*, February 8, 2025, https://www.rferl.org/a/russia-wagner-mercenaries-central-african-republic-crimes/33306858.html (accessed February 23, 2026).
[34] Mwambia, 'False'.

Mali. In Mali, military coups in 2020 and 2021 and the subsequent withdrawal of French forces created a security vacuum that the Wagner Group was quick to exploit.[35] Wagner's military engagement in Mali was reportedly worth USD10 million a month–a figure unsustainable for Mali's fragile budget.[36] This gave rise to speculation that Wagner might instead have been compensated through resource concessions, as Mali boasts vast reserves of gold, diamonds, lithium, manganese, silver, and other minerals, and companies such as Alpha Development and Marko Mining, allegedly linked to Wagner, have positioned themselves for such deals.[37] Although Mali's more centralized governance and better institutional stability (as compared to the CAR) have made it more difficult for Wagner to obtain direct access to the gold mining industry, Russia has pursued alternate approaches: lobbying for the nationalization of gold mines, leveraging anti-Western sentiment, and changing legislation to restructure the resource environment.[38] This illustrates how illicit enrichment, corruption, and opaque patronage are instrumentalized as hybrid tools to establish long-term influence.

China

The changing nature of warfare has also been noted by Chinese military leaders. In their 1999 book *Unrestricted Warfare*, People's Liberation Army Senior Colonels Qiao Liang and Wang Xiangsui argued that the fundamental principle of war was no longer 'using armed force to compel the enemy to submit to one's will' but was instead 'using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's interests.'[39] A new name would be needed for this '[w]arfare which transcends all boundaries and limits, in short: unrestricted warfare.'[40] With no restrictions, 'all means will be in readiness, … information will be omnipresent, and the battlefield will be everywhere.'[41]

The colonels recognized how this concept of unrestricted warfare implies a practically infinite choice of means ('[T]here is nothing in the world today that cannot become a weapon, and this requires that our understanding of weapons must have an awareness that breaks through all boundaries.'[42]) and a greatly expanded sense of threat ('The new concept of weapons will cause ordinary people and military men alike to be greatly astonished at the fact that commonplace things that are close to them can also become weapons with which to engage in war.')[43] This new kind of weaponry would not threaten imminent bodily harm, but it would nevertheless be effective in subjugating an opponent: '[T]he best way to achieve victory is to control, not to kill.'[44]

Invoking a Machiavellian logic, pursuing aims by any available means, the authors float a range of tactics, while noting the moral cost. These include psychological operations aimed at soldiers' families, assassinating financiers, pretextual 'surgical' strikes without a declaration of war, and acquiring media outlets to turn another country's news and television into instruments of propaganda.[45] They also consider directly influencing foreign governments through lobbying, asking whether 'special funds [can] be set up to exert greater influence on another country's government and legislature.'[46]

[35] Carl Michael Gräns, "*Russia's Growing Influence in Mali. Is Burkina Faso Next?*" (FOI Studies in African Security, January 2023), https://www.foi.se/rest-api/report/FOI%20Memo%208087.
[36] Kemal Mohamedou, *The Wagner Group, Russia's Foreign Policy and Sub-Saharan Africa*, Geneva Paper 32/24 (Geneva: Geneva Centre for Security Policy, March 2024), https://dam.gcsp.ch/files/doc/geneva-paper-32-2024.
[37] Ibid.
[38] Gleb Golubkov, "Gold and Crossbows: How Russian Mercenaries Support Dirty Russian Business in Africa?" Transparency International, July 3, 2025, https://ti-russia.org/en/2025/07/03/gold-and-crossbows-how-russian-mercenaries-enable-dirty-business-in-africa/.
[39] *Unrestricted Warfare*, p 7.
[40] *Id.* p. 12.
[41] *Id.*
[42] *Id.* p. 25.
[43] *Id.* p. 26.
[44] *Id.* p. 27.
[45] *Id.* p. 191.
[46] *Id.*

Regarding this use of 'special funds', Qiao and Wang reach back more than two thousand years to cite a notable Chinese precedent:

> [T]his practice was to be seen long ago in ancient China. In the war between the Chu and the Han at the end of the Qin Dynasty … Liu Bang gave Chen Ping a great deal of money in order to defeat Xiang Yu off the battlefield.[47]

The authors of *Unrestricted Warfare* do not explicitly address the use of bribery and corruption as potential weapons on an expanded global battlefield. But if the founder of the Han Chinese legendarily used extensive bribery to secure the loyalty of his men and to defeat a superior foe 'off the battlefield,' we should consider that the modern Chinese Communist Party might perceive that as an important lesson from history.

And it does. Pervasive corruption in China's Belt and Road Initiative (BRI), China's potent tool of geopolitical influence, has been widely reported. There is the Chinese role in Malaysia's 1MDB corruption scandal.[48] There are alleged bribes paid by state-owned China Harbor Engineering Company through intermediaries to Sri Lanka's former president Mahinda Rajapaksa, which ultimately resulted in China gaining control over a deep sea port in Hambantota that may potentially host a Chinese forward military base.[49] There is Bangladesh cancelling a BRI highway construction project and blacklisting CHEC over allegations of bribes being offered to Bangladeshi officials.[50]

It is difficult, if not impossible, to ascertain whether a specific instance of foreign bribery by Chinese state-owned companies or ostensibly private champions is undertaken for commercial or political reasons, especially given the Chinese military-civil fusion policy.[51] But when we see these and other corrupt activities, we must be sensitive to the possibility that they are undertaken not merely with an eye to commercial gain. Rather this is part of a wider-ranging strategy for conquest as articulated by China's military leadership in 1999.

The Future of Weaponized Corruption

We should expect weaponized corruption to play a more frequent and prominent role in non-military geopolitical confrontations. But it will also be used to prepare favourable conditions for eventually committing the first wave of armed forces, which the Russian military strategists call the 'initial period of war.'

Beyond the use of direct corruption–for example, a nation paying foreign officials to support and further its own cause–there is a further danger of which we must be mindful. The corruption of public officials, from whatever source, can over time give rise to a significant degree of public anti-corruption sentiment. This can, in principle, be considered a healthy response, but it can also be abused to further the aims of strategic corruption. Such sentiment can itself be weaponized to sow chaos and create 'an internal opposition' and 'a permanently operating front throughout the entire territory of the enemy state.'

---

[47] *Id.* at 203, n.16.

[48] Will Doig, "The Belt and Road Initiative is a Corruption Bonanza," *Foreign Policy*, January 15, 2019, https://foreignpolicy.com/2019/01/15/the-belt-and-road-initiative-is-a-corruption-bonanza/ (accessed February 23, 2026); Jonathan Hillman, "Corruption Flows Along China's Belt and Road," *Center for Strategic and International Studies*, January 18, 2019, https://www.csis.org/analysis/corruption-flows-along-chinas-belt-and-road (accessed February 23, 2026); Wade Shepard, "How China's Belt and Road Became a 'Global Trail of Trouble," *Forbes*, January 29, 2020. https://www.forbes.com/sites/wadeshepard/2020/01/29/how-chinas-belt-and-road-became-a-global-trail-of-trouble/?sh=25bad8fd443d (accessed February 23, 2026).

[49] Smruti S. Pattanaik, "Controversy over Chinese investment in Sri Lanka," *East Asia Forum*, June 5, 2015, https://eastasiaforum.org/2015/06/05/controversy-over-chinese-investment-in-sri-lanka/ (accessed March 17, 2026); Gabriel Honrada, "China's global military base strategy taking shape," *Asia Times*, June 14, 2024, https://asiatimes.com/2024/06/chinas-global-military-base-strategy-taking-shape/ (accessed March 17, 2026).

[50] "Bangladesh Blacklists Chinese Construction Firm, Cancels Highway Deal After Bribe Claim," *South China Morning Post,* January 18, 2018, https://www.scmp.com/news/asia/south-asia/article/2129493/bangladesh-blacklists-chinese-construction-firm-cancels-highway (accessed February 23, 2026).

[51] Executive Order 13959, "Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies," November 12, 2020, https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies.

Sustained societal frustration may spill over into unrelenting protest movements, destabilizing societies and upending the *status quo* when there is a deficit of public trust in governments. Examples are many:[52] the Arab Spring, Occupy Wall Street, the French yellow vest movement, the UK Brexit vote, Ukraine's anti-corruption and pro-Western Revolution of Dignity, anti-austerity and anti-COVID restrictions protests, Black Lives Matter protests, the precipitous collapse of Ashraf Ghani's corruption-mired government and the Afghan National Security Forces after the withdrawal of the U.S. and NATO forces.

None of these examples reveals foreign adversaries as an obvious driving force, but they do demonstrate the power of public discontent. The division and distrust created by these movements–whether in the movements themselves or in the potential backlash, organic or coordinated–provide rich opportunities for strategic subversion. To that end, the underlying corruption and any evidence of it could be authentic, fabricated by intelligence services, or even arranged as part of active measures with the help of pocket oligarchs, state-owned companies, corporate champions or organized crime. In addition to social media campaigns, the Pandora Papers, WikiLeaks and Guccifer 2.0-type disclosures, new hybrid warriors may seek to establish new or subvert existing anti-corruption and investigative organizations. This is similar to how the Soviet Union manipulated the global peace movement during the Cold War through puppet organizations such as the World Peace Council, secret funding and the penetration of non-aligned peace groups.

If such scenarios seem remote or far-fetched, there is nevertheless one thing of which we can be certain: corruption and anti-corruption sentiments elicit such strong and predictable motivations in individuals and masses that the generals of new unrestricted wars will undoubtedly seek ways to harness their power.

Conclusion

Though tactics have evolved with globalization, modern warfare and technological advances, hybrid influence–the use of non-traditional or unconventional activities to strategically exert influence–has roots dating back thousands of years. As global information and geopolitical environments have made societies easier to reach, opportunities for hybrid influence have become available on a wider scale than ever before. This has prompted states to abandon traditional rules, permanently changing the concept of warfare.

The resurgence of these tactics–including the weaponization of corruption–have allowed armed forces to punch above their weight and to defy assumptions about traditional military capabilities. In recent decades, autocratic states, including Russia and China, have successfully weaponized corruption and deployed disinformation in foreign states to sow chaos, create internal opposition, destabilize societies, and win the favour of influential political and military figures. This sort of hybrid influence is often used to create favourable conditions for military confrontation. Our own efforts to fight corruption must take into account these state-based sources and purposes of corruption—including the strategic exploitation of the very anti-corruption sentiment to which influence campaigns may give rise.

[52] Isabel Ortiz, Sara Burke, Mohamed Berrada, and Hernán Cortés, *World Protests: A Study of Key Protest Issues in the 21st Century* (New York: Friedrich-Ebert-Stiftung, 2022).

3. The Impact of Human Rights Violations on Operations

Dr. Grazvydas Jasutis

Introduction

In April 2021, NATO Foreign and Defence ministers decided to withdraw all Allied troops from Afghanistan. Following the fall of the Afghan government, NATO suspended all areas of cooperation with the country. NATO stated that any future Afghan government would have to adhere to Afghanistan's international obligations; safeguard the human rights of all Afghans, particularly women, children, and minorities; uphold the rule of law; allow unhindered humanitarian access; and ensure that Afghanistan never again serves as a safe haven for terrorists.[1] Human rights remain one of the pre-conditions for re-establishing cooperation with Afghanistan thus demonstrating the tremendous importance of the values and standards that NATO and Allied states respect. NATO's Founding Treaty signed on 4 April 1949 in Washington DC, refers to '*the principles of democracy, individual liberty and the rule of law'* in its preamble.[2]

As a multi-national military alliance charged with maintaining stability in the Euro-Atlantic area, NATO has engaged in various international crisis management operations and missions since its founding. Such operations have grown in number and complexity since the end of the Cold War. As of September 2021, NATO led operations in Kosovo and the Mediterranean. In 2018, it initiated a training mission in Iraq, which aims to develop the capacity of Iraq's security forces. It also supports the African Union and conducts air policing missions at the request of its Allies and assists in responding to the refugee and migrant crisis in Europe.[3]

Although parties to the missions and operations conducted by international communities remain bound by international human rights law and international humanitarian law, there is evidence that human rights violations have been committed by security forces while executing such missions and operations. The consequences are profound, foremost for those who have suffered from such human rights violations, but also for the credibility of the operations and the international community at large. For instance, in the days after the U.S.-led operation in Iraq, looters stormed the Iraq Museum and ransacked its vast collections and those artifacts brought in millions of dollars to fund the insurgency that targeted American soldiers.[4] Multilateral organizations, such as NATO and the UN, have developed various policies and guidelines, in particular focusing on the protection of civilians in the planning and conduct of military missions. Illustrative examples include the 2016 NATO Policy for the Protection of Civilians, which seeks to 'avoid, minimize and mitigate the negative effects that might arise from NATO and NATO-led military operations on the civilian population'.[5] Also, NATO's role is to support Allies' obligations towards cultural property and to embed cultural property protection into all phases of military operations, missions and activities, as well as in delivering education, training and exercises.[6] The policy reflects the commitment of the international community to mainstream human rights in international military missions and operations. They also demonstrate the acknowledgment that human rights violations can undermine operational effectiveness, create space for corruption and integrity issues to emerge, and as a result, undermine the legitimacy and functioning of national and international defence institutions.

---

[1] NATO, "NATO Allies decide to start withdrawal of forces from Afghanistan," December 14, 2021, https://www.nato.int/cps/en/natohq/news_183086.htm?selectedLocale=en (accessed February 23, 2026).
[2] NATO, "The North Atlantic Treaty," April 4, 1949. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.
[3] NATO, "Operations and missions: past and present," September 10, 2021, last updated July 30, 2025, https://www.nato.int/cps/en/natolive/topics_52060.htm (accessed February 23, 2026).
[4] Wilson Reid, "The illegal antiquities trade funded the Iraqi insurgency. Now it's funding the Islamic State," *Washington Post*, March 9, 2015, https://www.washingtonpost.com/posteverything/wp/2015/03/09/how-shady-art-dealers-help-fund-the-islamic-states-violent-insurgency/ (accessed February 23, 2026).
[5] NATO, "Human security," last updated August 30, 2024, https://www.nato.int/en/what-we-do/wider-activities/human-security (accessed February 23, 2026).
[6] Ibid.

The aim of this chapter is to explore the impact of human rights violations on international missions and operations. The research has three parts. The first part focuses on the general impact of human rights violations on operations. The second part analyses the application of three fundamental human rights in the context of international military missions and operations: the right to life; the right to liberty and security, and the prohibition of torture, inhuman or degrading treatment. It examines cases in which these rights may have been violated by security forces acting under the auspices of international military missions and operations, and highlights policies and strategies developed by NATO to prevent and respond to such violations. The third one concentrates on good practice, and outlines tools and strategies which, taken together, might reduce the chances of human rights violations in international military missions and operations. The article concludes that violations of human rights in international military missions and operations have serious consequences both for the victims of such violations, and for the efficacy of the missions and operations in question. They may lead to an increased risk of corruption and unethical behaviour: they may dissuade local communities and actors from sharing much-needed intelligence with multinational forces, undermine the credibility of the multinational force, and push local communities into the hands of belligerents.

While the author has chosen to focus on three rights, it must be acknowledged that these rights do not exist in isolation from others. The article relies on primary and secondary data. The author interviewed NATO and UN officials, international security experts and researchers and referred to his own operational experience. Primary data was triangulated with open-source secondary data. Several challenges were encountered during the research phase, most notably difficulty in obtaining access to classified operational documents. To navigate this, primary data was collected which allowed the author to address human rights issues in a more comprehensive manner.

General Impact of Human Rights Violations on Operations

Violations of human rights in international military missions and operations have serious consequences both for victims, and for missions and operations in question.

Unethical behaviour: rampant human rights violations, especially those committed with impunity, may create a culture in which unethical behaviour becomes accepted, or even encouraged. Such behaviour may take the form of bullying, harassment, or mistreatment by security forces against local populations. It leads to an inability to maintain discipline and a prevalence of unethical behaviour resulting in civilian casualties and reduced operational effectiveness. For instance, in April 1995, drunken Russian soldiers went on a rampage in Semashki (Chechnya), throwing grenades into cellars filled with women and children, killing more than 100 civilians.[7] This prompted many protests in Russia comparing the soldiers to Nazis. It also increased the insurgency in neighbouring villages.

Increased corruption risks and violence: in the context of sexual exploitation and abuse, security forces may demand sex or sexual favours from locals in return for the provision of food, money, or protection. This practice is commonly referred to as 'sextortion' and is understood as sexual exploitation and abuse for private gain and therefore can be understood as a form of corruption.[8] Security forces may attempt to bribe the families and communities of victims of collateral damage in order that they do not report such incidents to the media, or to local authorities. Sexual exploitation and abuse is detrimental to operational efficiency and it leads to the serious disruption of operational activities as can be seen by the UN decision to send home the entire Gabon military contingent deployed by the UN in the Central African Republic in 2021.[9] The notorious case of Russian Colonel

[7] "Chechen Town's Survivors Live Amid Ashes and Rubble of Russian Attacks," *ReliefWeb*, August 26, 1996, https://reliefweb.int/report/russian-federation/chechen-towns-survivors-live-amid-ashes-and-rubble-russian-attacks.
[8] Nancy Hendry, "Sextortion: Sexual offence or corruption offence?," Transparency International, April 14, 2020, https://www.transparency.org/en/blog/sextortion-sexual-offence-or-corruption-offence (accessed February 23, 2026).
[9] United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA). "Press Release (15 September 2021)." *ReliefWeb*. September 15, 2021. https://reliefweb.int/report/central-african-republic/press-release-15-september-2021 (accessed March 10, 2026)

Budanov (who raped and killed a Chechen girl during the war) further illustrates negative consequences.[10] The incident became a highly symbolic case in the Chechen conflict, reinforcing local perceptions of impunity and abuse by Russian forces. It intensified resentment among the Chechen population, and was widely used by insurgent groups to mobilize support and justify continued resistance. There were allegations of judges being bribed that brought about serious political repercussions, in addition to a blood feud and the subsequent death of Colonel Budanov. Human rights violations of the detained may be associated with increased corruption risks and may see detainees bribing correctional personnel or international forces in order to be released or in order not to be transferred to local authorities.

Damage to international credibility and operational effectiveness: human rights violations can tarnish the reputation of states and international organizations involved in international military missions and operations. On 7 April, 2022 UN members voted in favour of expelling Russia from the UN Human Rights Council after rampant violations of human rights in Ukraine.[11] When reported in the mass media, such violations can prompt governments, human rights activists and civil society organizations to demand policy changes, enhanced accountability. In extreme cases, violations have led nations to withdraw national contingents from international military missions and operations. Another case in point is the UN peacekeeping mission in Haiti, MINUSTAH. The UN peacekeepers, inadvertently, brought cholera to an island that had never in its history seen such a disease. The UN later struggled to acknowledge responsibility for this ethical and legal failure. Indeed, one UN Special Rapporteur would characterize the UN's handling of the issue as 'morally unconscionable, legally indefensible … politically self-defeating [and] entirely unnecessary.'[12] This shows how, even if no malice or criminal intent precedes a failure, the way an organization deals with the fallout is also a test of its own integrity. Further, human rights violations can damage the prestige of the military profession as a whole by tarnishing the credibility of the vast majority of security forces who act with honesty and integrity. The Russian Federation is considering announcing a total mobilization as its toxic war in Ukraine has damaged the prestige of the military profession and hindered its ability to generate new voluntary forces.

Reprisals and hearts and minds: local actors or communities may seek reprisals for human rights violations committed by an international military mission or operation. Such reprisals have been extensively documented when drone strikes were used during international military missions and operations which resulted in civilian casualties. To the same end, human rights violations, including illegal detention, mistreatment, sexual exploitation and abuse and collateral damage, can turn local communities and actors against multinational forces. NATO ISAF's ability to obtain intelligence information in Afghanistan (at Provincial Reconstruction Team level) was put at stake as civilian casualties dissuaded local communities and actors from sharing much-needed intelligence with multinational forces, and occasionally pushed local communities into the hands of belligerents.[13]

Budgetary cuts: once the credibility of an international military mission or operation is undermined, troop contributing countries may withdraw support. This might be either due to credible concerns about human rights violations, domestic political pressure, or a combination of both. This may also include cutting the funding necessary for the effective conduct of such missions, and the long-term funding necessary to stabilize a country once it emerges from conflict.

---

[10] Myers, Steven Lee. "Russian Colonel Convicted of Murdering Chechen Woman." *New York Times*, July 25, 2003. https://www.nytimes.com/2003/07/25/international/russian-colonel-convicted-of-murdering-chechen-woman.html (accessed March 10, 2026)

[11] United Nations General Assembly. "Suspension of the Rights of Membership of the Russian Federation in the Human Rights Council." Resolution A/RES/ES-11/3, 7 April 2022. https://digitallibrary.un.org/record/3967950 (accessed March 10, 2026)

[12] Philip Alston, "Statement by Professor Philip Alston, Special Rapporteur on extreme poverty and human rights UN responsibility for the introduction of cholera into Haiti," Office of the High Commissioner for Human Rights (OHCHR), October 25, 2016, https://www.ohchr.org/en/statements-and-speeches/2016/10/statement-professor-philip-alston-special-rapporteur-extreme.

[13] Beljan, Robert. *What Lessons Can Be Learned from ISAF for Future Peacekeeping Operations?* Peace Operations Training Institute, 2013

Analysis of the Selected Human Rights in the Context of Operations

1. Rape and Other Forms of Sexual Violence as Forms of Torture, Inhuman or Degrading Treatment

While various acts, not just sexual exploitation and abuse, may violate the prohibition of torture, inhuman or degrading treatment, sexual exploitation and abuse remain one of the most extreme forms of abuse of power. It is also one of the areas that international organizations, such as NATO and the UN, have invested significant efforts and resources in addressing.

Allegations have emerged that parties to international military missions and UN peacekeeping missions have committed sexual violence, exploitation and abuse against local populations. While no precise figures exist, the UN recorded over 2000 allegations of sexual abuse and exploitation by UN peacekeeping and other personnel between 2004–2016.[14] In 2015, the UN began publishing statistics on the nationalities of soldiers alleged to have sexually exploited and abused women and girls. According to these figures, an annual average of 77 complaints alleging sexual exploitation or abuse has been recorded since 2007. These allegations concern various peacekeeping missions, with the United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic (MINUSCA), the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO – formally the United Nations Mission in the Democratic Republic of Congo), the United Nations Mission in Liberia (UNMIL), the United Nations Operation in Côte d'Ivoire (UNOCI), and the United Nations Mission in South Sudan together accounting for the majority of reports.[15] Allegations of rape, sexual abuse of minors, and the use of sex workers by military forces emerged during the Kosovo Force (KFOR) and the Stabilisation Force in Bosnia and Herzegovina (SFOR).[16] Human Rights Watch found 'substantial' evidence that civilian contractors working under the auspices of SFOR regularly exploited the victims of sex trafficking, including under-age girls.[17]

Sexual exploitation and abuse are detrimental to international missions and operations. They tarnish the reputation and objectives of the operation. The UN mission in Haiti faced public anger over allegations that Uruguayan UN troops raped an eighteen-year-old local man, threatening the reputation of UN peacekeepers in the Caribbean state; the Haitian president Martelly acknowledged Haiti still needed the peacekeepers, but called for a redefinition of their future role and for the creation of a Haitian security force to eventually replace them.[18] The alleged perpetrators approached the family of the victim and tried to bribe them so they would not report the relevant incidents to the media, or to local authorities. This further aggravated the credibility of the operation and jeopardized the safety and security of peacekeepers on the ground. Sexual exploitation and abuse may affect the operational effectiveness and ability of peacekeepers to conduct their routine tasks. In September 2021, UN Secretary-General Antonio Guterres ordered, as noted above, the immediate repatriation of the entire Gabon UN peacekeeping contingent serving in the Central African Republic. This followed on from credible reports of sexual abuse by some of its 450 members and past allegations[19]. The departure of the entire contingent caused the mission to temporarily be unable to carry out routine tasks.

---

[14] Calculations compiled by the Code Blue Campaign, based on the annual SG's Special Measures Reports, Code Blue Campaign, 2004–2016, http://www.codebluecampaign.com/reports.
[15] United Nations, "Sexual exploitation and abuse."
[16] Ragnhild Nordås and Siri Camilla Aas Rustad, "Sexual Exploitation and Abuse by Peacekeepers: Understanding Variation," *International Interactions* 39, no. 4 (2013): 511-534.
[17] *Human Rights Watch, Hopes Betrayed: Trafficking of Women and Girls To Post-Conflict Bosnia and Herzegovina for Forced Prostitution*, November 26, 2002, https://www.hrw.org/report/2002/11/26/hopes-betrayed/trafficking-women-and-girls-post-conflict-bosnia-and-herzegovina.
[18] Joseph Guyler Delva, "U.N. Haiti peacekeepers face outcry over alleged rape," *Reuters*, September 6, 2011, https://www.reuters.com/article/uk-haiti-uruguay-un-idUKTRE7844HQ20110906 (accessed February 23, 2026).
[19] "UN withdraws Gabon peacekeepers from CAR after sex abuse claims," *France 24*, September 15, 2021, https://www.france24.com/en/africa/20210915-un-withdraws-gabon-peacekeepers-from-car-after-sex-abuse-claims (accessed February 23, 2026).

International organizations have made real efforts to address these issues. In 2004 NATO introduced the Policy against Trafficking in Human Beings (THB). The Policy included, amongst others, guidelines for NATO staff on preventing the promotion and facilitation of trafficking in human beings. The guidelines prohibited NATO staff, including consultants and temporary personnel, from engaging in THB activities, and obliged them to report known cases of THB involving NATO staff.[20] The adoption of this policy signalled recognition on the part of NATO of the enormous harm caused by the involvement of NATO staff in sexual exploitation and abuse, both to victims, and to the credibility of international military operations and missions conducted by NATO.[21] Some years later, in 2019, NATO adopted its first-ever policy to prevent and respond to sexual exploitation and abuse, which applies to all personnel and makes clear NATO's zero tolerance approach in this area.[22]

Box 3.1. The Approach of NATO to Preventing and Responding to Sexual Exploitation and Abuse

The NATO Policy on Preventing and Responding to Sexual Exploitation and Abuse was endorsed by NATO Ministers of Foreign Affairs on 20 November 2019. The Policy states that NATO is committed to the principles of individual liberty, democracy, human rights and the rule of law. It reiterates that NATO's Code of Conduct requires all staff to act with integrity, loyalty, accountability, impartiality, and professionalism. It notes that sexual exploitation and abuse run counter to NATO's principles and core values and undermine the effectiveness and credibility of the Alliance and risk mission success. It reaffirms that NATO has a zero-tolerance approach to all acts of sexual exploitation and abuse. The Policy is divided into two sections. The first addresses preventive measures and the second, reactive measures. The Policy notes that all personnel are prohibited from engaging in, or facilitating, any form of sexual exploitation and abuse; and must strive to prevent and respond to sexual exploitation and abuse within their sanctioned power and authority. It outlines that all personnel are to be vetted by the appropriate national authority based on national procedures and regulations in line with this Policy. As regards reactive measures, the Policy outlines that NATO will ensure that there are complaint mechanisms that enable alleged cases of Sexual Exploitation and Abuse to be duly and appropriately submitted to competent authorities by complainants. It notes that Nations are responsible for conducting investigations and pursuing appropriate administrative, disciplinary, or criminal proceedings related to allegations of sexual exploitation and abuse concerning their personnel. To this end, the Policy reaffirms that discipline over military and civilian personnel provided by member nations is a national responsibility.

Source: https://www.nato.int/cps/en/natohq/official_texts_173038.htm

2. Right to Life

The right to life is encompassed in most international and regional human rights instruments. In the conduct of operations during armed conflict, armed forces are bound by the provisions of the law of armed conflict that are designed to limit, as much as possible, the effects of war on those persons directly participating in hostilities and the objects they use to accomplish their military goals.[23] Accordingly, a set of rules governs who and what may be targeted by armed forces in military operations.[24] These rules reflect a fundamental compromise between military necessity and humanity. In all armed conflicts, civilians are protected from direct attack, 'unless and for such time as they take a direct part in hostilities.'[25]

[20] NATO, "NATO Policy on combating trafficking in human beings," June 29, 2004, https://www.nato.int/cps/en/natohq/official_texts_71856.htm?selectedLocale=en (accessed February 23, 2026).
[21] Alvaro Ballesteros, "Trafficking in Human Beings and International Peacekeeping Missions: the 2004 NATO THB Policy," *Connections: The Quarterly Journal* 6, no. 3 (2007): 121-139, http://connections-qj.org/system/files/06.3.08_ballesteros.pdf.
[22] NATO, "NATO adopts first-ever policy on preventing and responding to sexual exploitation and abuse," September 18, 2020,' https://www.nato.int/cps/en/natohq/news_173057.htm?selectedLocale=en (accessed February 23, 2026).
[23] *Handbook on International Rules Governing Military Operations* (Geneva: International Committee of the Red Cross, 2013), https://www.icrc.org/sites/default/files/topic/file_plus_list/0431-handbook_on_international_rules_governing_military_operations.pdf.
[24] Ibid.
[25] Ibid.

Civilian casualties remain a major concern for the international community and NATO. In Afghanistan the researchers found strong evidence that local exposure to civilian casualties caused by international forces leads to increased insurgent violence over the long-run. This is sometimes termed the 'revenge' effect.[26] There are different actors on the ground that directly or indirectly participate in the conflict and their actions inflict civilian casualties. The activities and role of private military and security companies (PMSCs) became a major concern for the Afghan government, both because of these links and because ISAF forces permitted security contractors to use deadly force not only in self-defence, but also to protect military installations and convoys. The protection of military logistic convoys along the route between Kabul and Kandahar, for example, embroiled private security guards in firefights with groups of up to 200 insurgents.[27] The UK's former commander in southern Afghanistan, Major-General Nick Carter, warned that PMSCs operated in a 'culture of impunity'.[28]

NATO in particular was also concerned about civilian casualties in Afghanistan. In June 2008, shortly after General David McKiernan assumed command, ISAF was involved in two high profile incidents resulting in numerous civilian casualties.[29] As described in a 2008 UNAMA report, '[incidents included] a number of high-profile cases, including air strikes carried out in Deh Bala district in Nangahar Province on July 6, 2008 which resulted in the deaths of 47 civilians, including 30 children'.[30] Information on these events from local NGOs, the Taliban, and international organizations differed so dramatically from ISAF's data that ISAF recognized the need for action.[31] Implemented in 2008, the Civilian Casualty Tracking Cell was created within ISAF to collect data on civilian casualties. This mechanism resulted in the issuance of new tactical directives and guidelines by ISAF and NATO in an effort to mitigate casualties among civilians.[32] As a result, civilian casualty rates caused by pro-government forces significantly dropped in the following year.

In 2009 the new commander of ISAF, U.S. General Stanley McChrystal, declared the protection of civilians the main goal of the mission. On 6 July 2009 he issued the tactical directive, which stated that 'I expect all levels to scrutinize and limit the use of force like close air support against residential compounds and other locations likely to reduce civilian casualties in accordance with this guidance. Commanders must weigh the gain of using close air support against the cost of civilian casualties, which in the long run make mission success more difficult and turn the Afghan people against us'.[33] As a matter of fact, civilian casualties and human rights violations fuel insurgency and slow down operational tempo. This may dissuade such communities and actors from sharing much-needed intelligence with multinational forces, undermine the credibility of the multinational force, and push local communities into the hands of belligerents.

Furthermore, civilian casualties may mobilize the international community to act against your forces. The invasion of Ukraine by the Russian Federation (RF) began on 24 February 2022, with the end-goal being to bring about regime change in Kyiv and 'legitimize' the annexation of Crimea, the Donetsk People's Republic and the Luhansk People's Republic. The initial phase of the invasion by the RF did not result in the achievement of significant military objectives, therefore the military aggression led to an intensification of the targeting of civilian infrastructure by the RF, civilian casualties and grave violations of international humanitarian law. For instance, Russian forces occupied Bucha and Human Rights Watch found extensive evidence of summary executions, other unlawful killings, enforced disappearances, and torture, all of which would constitute war crimes and potential

[26] Luke N. Condra, Joseph H. Felter, Radha K. Iyengar et al., "The effect of civilian casualties in Afghanistan and Iraq," Working Paper 16152, National Bureau of Economic Research, July 2010, https://www.nber.org/system/files/working_papers/w16152/w16152.pdf.
[27] Elke Krahmann, "NATO contracting in Afghanistan: the problem of principal–agent networks," *International Affairs* 92, no. 6 (2016): 1401-1426.
[28] Ibid.
[29] *Civilian Harm Tracking: Analysis of ISAF Efforts in Afghanistan*, (Washington, DC: Center for Civilians in Conflict, 2014), https://civiliansinconflict.org/wp-content/uploads/2017/09/ISAF_Civilian_Harm_Tracking.pdf.
[30] *Armed Conflict and Civilian Casualties, Afghanistan, Trends and Developments 1 January - 31 August 2008*, (UNAMA, September 10, 2008), www.ohchr.org/Documents/Countries/Armed%20ConflictCivilianCassualties2008.pdf.
[31] *Civilian Harm Tracking: Analysis of ISAF Efforts in Afghanistan*.
[32] *Afghanistan, Implementation of a Civilian Casualty Tracking Cell*, (Geneva: International Committee of the Red Cross), http://ihl-in-action.icrc.org/case-study/afghanistan-implementation-civilian-casualty-tracking-cell.
[33] NATO "ISAF Tactical directive," July 6, 2009.

crimes against humanity.[34] The images from Bucha increased the moral pull to aid Ukraine in its war of self-defence and to support its efforts to defeat Russia through additional military assistance, sanctions, and accountability.[35] Before the war began, three countries were substantially assisting Ukraine with defence equipment, and that number has now risen to thirty-five.[36]

NATO continues to pay significant attention to civilian casualties and human rights. NATO policy states that lack of consideration for Protection of Civilians (POC) or PoC-related issues will have a negative impact on the overall mission and will hinder considerations of the root causes of the conflict or crisis, jeopardizing its success and long-term stability in the conflict or crisis area.[37] PoC considerations are an integral part of all crises and conflicts, even when a NATO mission does not have an explicit PoC mandate provided by the North Atlantic Council (NAC) that encompasses all aspects of the PoC concept.[38]

From a military professional perspective, the mitigation of harm to civilians is one of the three prongs of the so-called 'combatant's trilemma' between mission accomplishment, protection of one's own forces, and avoiding harm to civilians.[39] Constitutive and contingent factors may further illuminate this trilemma. The first refer to the very essence of the military profession, the concept of 'unlimited liability' (for example, the ethos of the Canadian Armed Forces: https://forces.ca/en/values-ethos/. Contingent factors refer to the kind of mission/deployment in a given situation (for example, a peacekeeping or humanitarian mission may require an even higher standard of protection for civilians than traditional warfighting missions).

Box 3.2. Good practice: NATO Policy for the Protection of Civilians

At the Warsaw Summit in July 2016, NATO leaders endorsed the NATO Policy for the Protection of Civilians. NATO recognizes that all feasible measures must be taken to avoid, minimize and mitigate harm to civilians. When planning and implementing such measures, NATO should give consideration to those groups most vulnerable to violence within the local context.

In the planning and conduct of military operations and missions, NATO will continue to take measures, including institutionalizing civilian harm mitigation measures, based on lessons learned and best practices. NATO will also continue to inquire of local authorities, populations and civil society, for example relevant organizations working for human rights, including gender equality, as to the most suitable and effective harm mitigation activities in the local context. Civilian harm mitigation measures should be developed and incorporated in NATO Command Structure and NATO Force Structure processes.

NATO offers a number of activities that support the implementation of POC, including training of local forces, defence and related security capacity building, partnership tools and programmes that make use of partner programmes, tools and mechanisms and include PoC-related objectives as part of their partnership goals and objectives. At the Brussels Summit in June 2021, Allied Leaders committed to continue working with partners, international organizations and civil society to further NATO's work on human security, including the protection of civilians.

Source: https://www.nato.int/cps/en/natohq/official_texts_133945.htm

[34] *Human Rights Watch*, "Ukraine: Russian Forces' Trail of Death in Bucha," April 21, 2022, https://www.hrw.org/news/2022/04/21/ukraine-russian-forces-trail-death-bucha (accessed February 23, 2026).
[35] Dan Baer, "Bucha Increases the Moral Pull for the West to Aid Ukraine," *Carnegie Endowment for International Peace*, April 5, 2022, https://carnegieendowment.org/russia-eurasia/posts/2022/04/bucha-increases-the-moral-pull-for-the-west-to-aid-ukraine (accessed February 23, 2026).
[36] Ibid.
[37] NATO, *Protection of Civilians: ACO Handbook* (2019), https://share.google/hs5JGTaxFfL6fmlgb.
[38] Ibid.
[39] Andrew Bell, "Combatant socialization and norms of restraint: Examining officer training at the US Military Academy and Army ROTC," *Journal of Peace Research* 59, no. 2 (2022): 180-196, https://journals.sagepub.com/doi/10.1177/00223433211010861.

3. Human Rights Violations in Detention Facilities

Detention is often necessary in multinational operations to ensure that the force is able to carry out its mandate, act in self-defence and protect the local population.[40] In conflict-affected areas, the fundamental principle that governs detention and internment is that every person has the right not to be subjected to arbitrary deprivation of liberty.[41] This means that there must be a legal basis for detention in the national law of the state and/or in the law of armed conflict. The deprivation of liberty of a particular person in any particular case must be based on good legal grounds and carried out in accordance with procedures laid down by law. Another important principle of the law of armed conflict is that persons detained by a party to an armed conflict must be treated humanely, and are entitled to certain fundamental guarantees.[42]

In multi-national operations, detention used inappropriately can lead to the mistreatment of members of the local population and a loss of international and national support for the multinational force, as well as criminal and disciplinary charges against those who have mistreated detainees.[43] It can also result in claims being brought against the governments comprising the multinational force regarding their responsibility for the breach of human rights and/or international humanitarian law norms.[44] In limited circumstances, this can also include claims against a multinational force, to the extent that it constitutes an international organization with independent legal responsibility that exercises effective control over the conduct of its troop contingents.[45]

While there are stark legal and political challenges related to the detention of persons in multi-national operations, one of the most important aspects is the transfer of detainees to local authorities where they may be exposed to an increased risk of torture, inhuman and degrading treatment, or to forced disappearances. It is worth noting that the rules of engagement of the NATO-led ISAF operation permitted the detention of individuals captured on the battlefield or in counter-terrorism operations. But prisoners had to be released or otherwise transferred to the custody of Afghan authorities within 96 hours. ISAF rules also stated that, consistent with international law, persons should not be transferred if there is a risk that they will be subjected to torture or other forms of ill-treatment.[46] The transfer of detainees to local authorities and the rights of states that hand over detainees were further discussed during the Copenhagen Process.[47]

Human rights violations in detention facilities have been well documented in conflict-affected countries. Serious issues in detention facilities were observed in Afghanistan. For instance, from October 2010 to August 2011, the United Nations Assistance Mission in Afghanistan (UNAMA) found compelling evidence that 125 detainees (46 % of the 273 detainees) interviewed who had been in National Directorate of Security (NDS) detention had been mistreated. They had experienced interrogation techniques at the hands of NDS officials that amounted to torture, and torture, UNAMA concluded, had been practised systematically in a number of NDS detention facilities in Afghanistan.[48] The findings of the investigation suggest that multinational forces and coalitions should take into consideration the situation on the ground and stop transferring detainees to local authorities where they could face torture or mistreatment. The prohibition of torture, it should be remembered, is a rule that has reached the status of a *jus cogens* norm of international law.

---

[40] Bruce Oswald, "Some controversies of detention in multinational operations and the contributions of the Copenhagen Principles," *International Review of the Red Cross* 95, no. 891/892 (2013): 707–726, https://international-review.icrc.org/sites/default/files/irrc-891-892-oswald.pdf.
[41] *Handbook on International Rules Governing Military Operations* (Geneva: ICRC, 2013).
[42] Ibid.
[43] Oswald, "Some controversies of detention in multinational operations."
[44] Ibid.
[45] Ibid.
[46] *Treatment of Conflict-Related Detainees in Afghan Custody* (UN, October 2011), https://unama.unmissions.org/sites/default/files/october10_2011_unama_detention_full-report_eng.pdf.
[47] *The Copenhagen process on the handling of detainees in international military operations* (International Institute of Humanitarian Law, 2018), https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/Copenhagen-Process-Principles-and-Guidelines-EN.pdf.
[48] *Treatment of Conflict-Related Detainees in Afghan Custody.*

In this context, it is worth referring to the case of Canada. Canadian troops began transferring detainees to Afghan authorities in late 2005.[49] On 18 December 2005, an Arrangement for the Transfer of Detainees between the Canadian Forces and the Ministry of Defence of the Islamic Republic of Afghanistan was signed. The arrangement established procedures in the event of a transfer, from the custody of the Canadian Forces to the custody of any detention facility operated by the Islamic Republic of Afghanistan of any detainee in the temporary custody of the Canadian Forces in Afghanistan.[50] The participants committed to treat detainees in accordance with the standards set out in the Third Geneva Convention. Eventually, faced with newspaper stories and other allegations of abuse in early 2007, the Canadian military temporarily suspended transfers.[51] On 3 May 2007 an Arrangement for the transfer of detainees between the Government of Canada and the Government of the Islamic Republic of Afghanistan was signed, which introduced a monitoring mechanism for detainees transferred to the Afghan authorities. Nevertheless, allegations of abuse and torture continued, and Ottawa decided to stop transfers.[52] A House of Commons special committee was established, and the Military Police Complaints Commission opened an inquiry into whether Canadian military police should have started criminal enquiries against members of Canadian forces involved in transfers in Afghanistan.[53] NATO, in a sweeping July 2011 directive, ordered all units to cease handovers to the notorious Afghan intelligence service, the National Directorate of Security, and to the Afghan National Police and Afghan Border Police.[54] All in all, Canada's experience here demonstrates the need to establish robust monitoring regimes for the detainees transferred to local authorities and to ensure regular monitoring.

The violations of the human rights of detainees can be associated with increased corruption risks as well. For example, detainees may attempt to 'bribe' correctional personnel in order to prevent mistreatment, or to secure early release. In cases where detention facilities are managed and staffed by local security forces, such forces may attempt to encourage international forces to 'turn a blind eye' to abuse by offering bribes. In other cases, international forces may accept bribes from victims of human rights violations in order that they not be transferred to local detention facilities. Victims may bring claims against troop-contributing countries for human rights violations committed by security actors operating (or with the inability to protect human rights) under the auspices of an international military mission or operation. In certain circumstances, this can also include claims against the multinational force, to the extent that it constitutes an international organization with independent legal responsibility that exercises effective control over the conduct of troop contingents.

Good Practice in Reinforcing Human Rights Protection in Operations

The protection of human rights in operations, and addressing the interface between human rights violations and corruption, remains of utmost importance. From DCAF's perspective, it can mainly be achieved through four main activity lines:

- **Provision of legal, policy and technical advice** on how to develop and implement human rights, anti-corruption, and gender frameworks, policies, and programmes. It is important to integrate human rights and gender perspectives into an operation's mandate. A human rights perspective should also be included when drafting and applying operational documents and mission policies. This framework ought to include an elaboration of the links between human rights violations and increased corruption risks, and should be accompanied by a comprehensive action plan to address such linkages. High level security policy documents need to be adjusted in order to reflect this kind of a framework. For instance, a clear

[49] David Ljunggren, "Canada generals deny ignoring Afghan abuse warning," *Reuters*, November 25, 2009, https://jp.reuters.com/article/canada-generals-deny-ignoring-afghan-abuse-warning-idUSN25196651/.
[50] *Afghanistan/Canada, Agreements on the Transfer of Detainees*, (Geneva: International Committee of the Red Cross), https://casebook.icrc.org/case-study/afghanistancanada-agreements-transfer-detainees.
[51] Ljunggren, "Canada generals deny ignoring Afghan abuse warning."
[52] Allan Woods, "Canada halts transfer of Afghan detainees," *Toronto Star*, January 24, 2008, https://www.thestar.com/news/canada/2008/01/24/canada_halts_transfer_of_afghan_detainees.html (accessed February 23, 2026).
[53] Marco Sassòli and Marie-Louise Tougas, "International Law Issues Raised by the Transfer of Detainees by Canadian Forces in Afghanistan," *McGill Law Journal*, Volume 56, Number 4, (June 2011): 959–1010.
[54] "NATO order ended Canadian transfer of Afghan prisoners," *CBC News*, June 11, 2012, https://www.cbc.ca/news/politics/nato-order-ended-canadian-transfer-of-afghan-prisoners-1.1263740 (accessed February 23, 2026).

framework is needed to address challenges related to the transfer of detainees to local authorities, including the increased risk of exposure to torture, inhuman or degrading treatment; to forced disappearances or to corruption among detention personnel. The provision of advice to local authorities on the treatment of detainees and the establishment of a robust monitoring mechanism in case of transferred detainees should contribute to the protection of human rights policies. The full implementation of the NATO Policy for the Protection of Civilians, as well as its periodic monitoring to respond to new challenges in the planning and conduct of operations, is essential. As regards sexual exploitation and abuse, NATO has adopted a zero-tolerance approach to all acts of sexual exploitation and abuse and aims to instil a coherent, consistent, and integrated approach and a strategic level framework to prevent and respond to sexual exploitation and abuse across NATO. Nevertheless, the effective implementation of such policies, as well as their constant monitoring, is required. For instance, at the individual level, there is a need to integrate a human rights component in performance-related processes and at organizational level, to develop a system to prevent the re-employment of personnel previously involved in human rights violations.

- **The development of capacities at the individual, organization and state levels** as regards the implementation of human rights, anti-corruption, and gender frameworks. Pre-deployment training on human rights, gender and ethics should be provided to both civilian and military personnel, including senior commanding staff.[55] This training should also focus on the interface between human rights violations and increased corruption risks in the context of international military missions and operations. Periodic training for civilian and military personnel is to be provided during missions and operations, and capacity building for local security actors on the protection of civilians and human rights should be offered. It is also essential that the capacity of oversight bodies, including ombuds institutions and general inspectorates, is further developed.

- **The promotion of norms, standards and good practices** related to the implementation of human rights, gender, anti-corruption, and ethics. This should stress the need for the Mission's leadership, including political and legal advisers, to engage with local and national authorities, civil society, the international community, and national governments in order to prevent violations of human rights and corrupt or unethical behaviour. Legal advisers should systemically monitor, investigate, document and report on the human rights situation in their area of responsibility and, when necessary, provide recommendations for corrective actions. Such recommendations should also address the interface between human rights violations and corruption. International organizations should mainstream a human rights perspective in their humanitarian responses to crises and armed conflicts and in post-conflict reconstruction activities.

- **The creation of knowledge products, toolkits, and guidance material** on the interface between human rights violations and corruption; their translation into relevant languages and their dissemination to key stakeholders. For instance, the application of NATO's Policy for the Protection of Civilians, and for Preventing and Responding to Sexual Exploitation and Abuse should be expanded and supplemented with additional information on corruption risks stemming from human rights violations. In addition, monitoring and evaluation material should be developed so the policy implemented can be assessed, and where necessary, amended.

[55] It is worth noting here the difference between 'training' and 'education'. While 'the two terms are often used interchangeably, training and education are both vital and represent different processes which are aimed at creating different outcomes. Training equips one to deal with the specifics; education that leads to reflective, deliberative thinking is required to allow the flexibility to adapt to the uncertainties of the real world' David Whetham, 'Special Operations Command: Leadership and Ethics Review,' in *Afghanistan Inquiry Report*, Inspector-General of the Australian Defence Force (Canberra: Commonwealth of Australia, 2020), pp. 504-531. Further: 'Ethics education needs to deal with complexity and ambiguity as opposed to values and standards training and/or law of armed conflict briefs, which focus very much upon right and wrong answers in specific black and white situations': David Whetham, 'Ethics and the Special Forces,' *In-Depth Briefing-CHACR 55* (2023), p. 2.

Conclusion

NATO and the international community have taken significant steps to improve protection for civilians and respect for human rights during armed conflicts. But the full integration of a human rights perspective in the planning and conduct of operations, constant monitoring and reporting on violations, a robust complaints system, not to mention periodic training for national and international forces need all to be in place.

Human rights violations committed during international military missions and operations have consequences that extend far beyond the immediate harm inflicted on victims. As this chapter has demonstrated, such violations can undermine operational effectiveness, weaken discipline and integrity within military forces, and create environments in which corruption and unethical behaviour flourish. They also damage the credibility of multinational missions, erode public and international support, and risk alienating local populations whose cooperation is often essential for mission success. In extreme cases, violations may fuel insurgency, provoke reprisals, or disrupt operational capabilities through the withdrawal of troop contingents or political support.

The chapter has highlighted that NATO has made significant progress in developing policies, frameworks, and operational tools aimed at preventing and responding to such violations. Initiatives such as NATO's Protection of Civilians policy, its policy on preventing and responding to sexual exploitation and abuse, and improved monitoring mechanisms demonstrate a growing recognition that respect for human rights is not only a legal and moral obligation but also a strategic necessity.

Part 2: The Comprehensive Approach to Building Integrity

This part of the Compendium turns toward solutions, showing how NATO's Building Integrity programme evolved into a comprehensive strategy for safeguarding defence institutions against corruption. It outlines NATO's original strategic approach, centred on integrity, transparency, and accountability, and explains how increasing defence budgets and technological change demand renewed governance and innovation. Another contribution shows how this framework matured into a wider culture of democratic oversight, multistakeholder cooperation, and institutional learning, positioning integrity as a security enabler rather than purely an anti-corruption tool. Finally, the third article explores how these principles translate into military practice through NATO's Military Concept for Building Integrity in Operations, demonstrating how corruption undermines missions and why embedding ethical safeguards into planning, execution, and assessment is essential for success. In combination, these contributions form a comprehensive approach that links governance reform, institutional design, and operational effectiveness.

4. A Strategic Approach for Improving Defence Integrity: Legal, Ethical, and Governance Perspectives

Prof. Todor Tagarev and Prof. Francois Melese

NATO's Building Integrity programme, launched nearly two decades ago, contributed to national efforts to reduce corruption in defence by complementing compliance- and ethics-based measures with enhanced transparency and accountability at individual and organizational levels. This 'strategic approach' has proved its worth. Yet, in conditions of large-scale war in Europe, substantial increases in defence budgets, shorter innovation cycles, and hybrid influence by malign actors, defence corruption remains a challenge. This chapter summarizes the original strategic approach and extends it by setting counter-corruption efforts in a wider good governance and defence management framework and outlining the benefits of advanced technologies for strengthening defence integrity.

Introduction

NATO launched its Building Integrity (BI) programme in 2007. Championed by heads of state and government [1] and military leaders, this broad support underpinned efforts by members and partner countries to better understand the impact of corruption in defence establishments. Practical tools and processes developed by NATO, in cooperation with other organizations, have assisted countries to assess corruption risks [2] and mitigate those risks.

Notwithstanding the significant achievements of countries that implemented the BI programme, many of which are discussed in this volume, persistent problems remain. These residual corruption risks could impact both combat preparedness and the effectiveness of the Alliance. Examples include:

- weakened operational readiness due to equipment shortfalls, delayed delivery, or inappropriate or faulty materiel reducing combat capability;
- unauthorized technology transfers that compromise operational security and reduce technological advantages of the Alliance and its partners;
- distortion of personnel hierarchies from nepotism or bribes for favourable positions or promotions, which can undermine unit cohesion; or
- diversion of mission funds that empower hostile actors.

Perhaps most damaging is how news of corruption spreads. Not only does it risk compromising missions, but it can undermine the legitimacy of operations in the eyes of soldiers, local populations, and nations.

There are specific vulnerabilities in the defence sector such as the large budgets involved, the need for secrecy, and the complexity of weapon systems. NATO members recently pledged to increase their defence and related security budgets to 5 % of GDP. This will boost NATO defence spending well above the USD1.3 trillion expended in 2025. This massive investment makes tackling corruption especially critical. Combined with stubborn budget deficits, high debt loads, and increasingly rapid product cycles, this creates challenges that require new and innovative solutions. Addressing corruption is therefore essential for protecting the Alliance's credibility and effectiveness.

[1] Bucharest Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, *Press Release* 2008(049), April 3, 2008, https://www.nato.int/cps/en/natolive/official_texts_8443.htm.
[2] See, for example, the section on the 'Self-Assessment and Peer Review Process' and the link to the 'Self-Assessment Questionnaire' at "Building Integrity," last updated January 22, 2025, https://www.nato.int/cps/en/natohq/topics_68368.htm (accessed January 1, 2026); and TI's Government Defence Integrity and Defence Companies indexes, https://ti-defence.org/what-we-do/industry-integrity/defence-companies-index/.

The search for savings to lower debt loads is likely to target national defence. To preserve Alliance capabilities, NATO's smart defence concept encourages collaboration between nations, and between nations and industry. This is explored further in Chapter 11. Closer collaboration between defence establishments, industry, and academia is essential for speeding up innovation and for maintaining NATO's technological and industrial edge, especially in new fields such as artificial intelligence, robotics, hypersonic technologies, etc.[3]

NATO's Building Integrity (BI) programme represents a critical initiative across the Alliance that helps address corruption risks within defence and security institutions. However, as member nations implement new measures, a fundamental tension has emerged: how to strengthen anti-corruption safeguards without compromising operational efficiency and without creating bureaucratic paralysis.

Defence organizations today face rapidly evolving threat environments that require agility, responsiveness, and resilience. So, for example, if anti-corruption measures slow capability development or procurement timelines, this may inadvertently compromise national security objectives. The challenge, therefore, is not whether to implement anti-corruption measures, but how to do so in a manner that complements and enhances institutional effectiveness and ensures resilience.

As much as possible, BI measures should be integrated into existing processes rather than added as additional layers. This requires careful analysis of current procedures to identify where integrity risks are highest and where controls can be most cost-effectively embedded. The goal should be to strengthen present-day processes rather than to create entirely new or parallel systems.

In their bid to minimize the harmful effects of corruption, defence organizations must first and foremost address organizational culture, professional norms, and individual incentives that influence behaviour. This cultural dimension requires long-term leadership engagement, and an ongoing commitment at all levels to build integrity, increase transparency, and improve accountability. Defence institutions legitimately need to protect sensitive information for operational security. Yet anti-corruption efforts often require access to such information. The challenge is to establish clear protocols that respect both sets of requirements.

Minimizing corruption risks within NATO member states represents a necessary goal for preserving the credibility and effectiveness of the Alliance. With new commitments by countries to substantially increase defence budgets, failure to tackle corruption could have enormous cost implications, and undermine operational readiness, strategic deterrence, and resilience. Fortunately, the emergence of sophisticated AI technologies provides new and unprecedented opportunities to combat these threats through intelligent oversight, predictive analysis, and automated transparency mechanisms.

The 2010 Compendium of Best Practices was among the first NATO BI products to recommend treatments for corruption risks identified and diagnosed by countries that completed the BI self-assessment questionnaire.[4] Chapter 2 of the Compendium offered a "strategic approach" and framework to minimize corruption that involves building integrity, increasing transparency, and improving accountability. The approach is based on a combination of ethical and utilitarian perspectives that focuses on individual incentives. The aim is to reduce the benefits to an individual of engaging in corrupt behaviour, and to increase the costs.

The current chapter extends this strategic framework by setting counter-corruption efforts in a wider good governance and defence management framework. The next section briefly summarizes the original approach. This is followed by the development of a national and institutional building integrity framework. The aim of said framework is to involve and empower all key stakeholders, limit individual discretion, develop important checks and balances, while increasing transparency and accountability to improve security outcomes and performance over time. The final section offers practical guidelines for the design and implementation of carefully crafted

[3] Todor Tagarev, Raphael Perl, and Valeri Ratchev, "Recommendations and Courses of Action: How to Secure the Post-Covid Future," in *Transatlantic Security: Securing the Post-Covid Future*, edited by IBM (Wien: Federal Ministry of Defence, 2020), pp. 18-41.
[4] Todor Tagarev, ed., *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO/DCAF, 2010), https://www.nato.int/cps/en/natohq/topics_104893.htm.

national and institutional BI programmes, including the potential application of advanced technologies to counter corruption.

A Strategic Approach to Counter Corruption

There is ample, if unfortunate, evidence that people with high discretionary power and low accountability can be tempted by the perceived benefits of corrupt activities. Those benefits can take the form of monetary or non-monetary rewards. Monetary benefits involve financial gains obtained *by abusing a position of trust or responsibility*, for example, abusing control over budgets, procurements, personnel, intelligence, or operations. Expected benefits can involve direct bribes, kickbacks, fraudulent (inflated) invoicing, false contracting, fake subcontractors, phantom services, shell companies, diverting equipment or supplies for resale, insider trading, or extracting promises of outside employment in exchange for favours.

Non-monetary benefits often involve a desire for power and influence that can also motivate corrupt behaviour. This may include the desire for more prestige, a more satisfying job, promoting a personal ideology, privileged access to sensitive information, perks (vehicles, housing, travel) to elevate social standing, securing leverage over superiors or peers through reciprocal favours, gaining influence outside the chain of command, or rewarding close associates, friends, or family with promotions, or favourable appointments or postings (patronage). Box 4.1 provides definitions of selected types of corrupt behaviour.

The strategic approach to minimize corrupt behaviour introduced in the 2010 Compendium recommends reducing expected payoffs. The aim is to shift the cost-benefit calculation for potential wrongdoers to make corruption less attractive. This involves two broad levers: 1) Reducing the perceived advantages (i.e., lower the 'marginal benefits'), and/or 2) Increasing the perceived risks (i.e., increase the 'marginal costs'). Susceptible individuals have an incentive to weigh the expected gains from illicit activity, against their own moral compass and the expected costs (i.e. the probability of detection, and anticipated punishment). Figure 4.1 illustrates how reducing the anticipated rewards of corrupt behaviour and increasing the expected costs can lead to fewer cases of corruption.

As articulated in the BI framework, an effective anti-corruption strategy must integrate three complementary pillars: ethical/moral considerations (*building integrity*) organizational/managerial dimensions (*increasing transparency*); and legal/economic factors (*improving accountability*). BI raises the moral or internal cost of corruption to the individual. Increasing transparency raises the probability that corrupt actions will be detected. Improving accountability ensures sanctions are credible and enforced, and that economic and/or other serious consequences are imposed for corrupt behaviour.

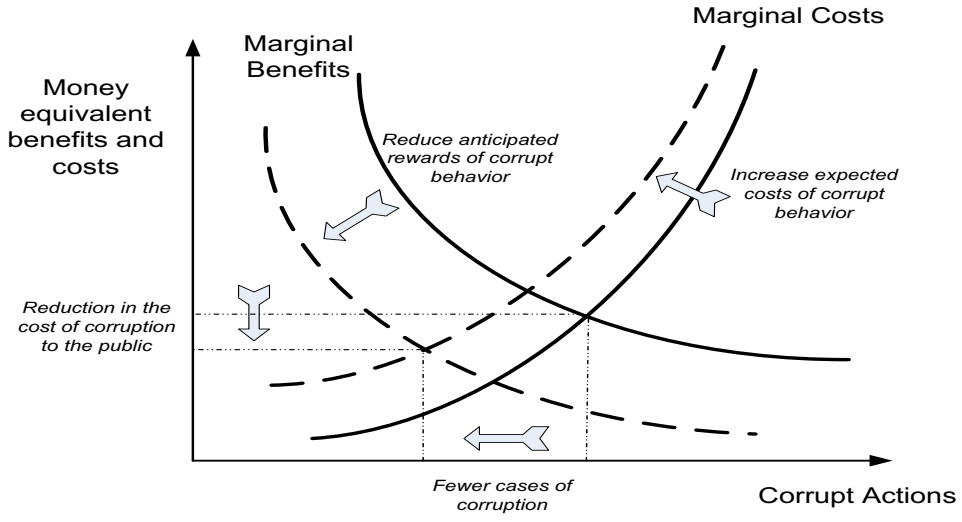


Figure 4.1: Foundations of the Strategic Approach to Reducing Defence Corruption.

Box 4.1 Examples of Corruption – 'the Misuse of Public Office for Private Gain' [5]

Embezzlement: Stealing or misusing public funds, property, products, supplies, or services

Bribery: Illegal payment, or a promise for payment made by a vendor to a public official to influence defence contracts

Extortion/graft: A public official demands a payment from a vendor to influence decisions on a defence contract or its implementation

Patronage: A public official awards favours, such as contracts, promotions, or assignments in return for political support

Nepotism: A public official awards special favours to family and friends NOT on the basis of merit/ performance

Building the integrity of individuals can be accomplished through various means including: ethics training, setting high expectations, clear codes of conduct, enacting military and civil service values, merit-based promotions and assignments, and most importantly, creating an ethical culture in the defence organization.

Box 4.2. Examples of Enhancing Transparency Measures in Budgeting and Procurement

Effective BI implementation means incorporating transparency at each stage of decision-making and management, such as:

- Publishing budget and procurement data online to allow near real-time monitoring and external scrutiny, which has been shown to reduce fraud and maintenance costs with minimal disruption to existing operations.
- Automating controls and reporting leveraging AI, for example by linking financial and resource allocation data platforms, which enables more efficient compliance checks without imposing slow manual processes.
- Simplifying procedures so that anticorruption requirements are integrated into routine forms and workflows, rather than as additional, duplicative paperwork.

For example, relatively low-cost automated contract analysis programmes leveraging AI could be deployed to analyse contracts for:

- Unusual pricing patterns relative to market benchmarks.
- Specification changes that favour particular vendors.
- Timeline modifications that benefit specific contractors.
- Contract language that creates unfair competitive advantages.

Finally, applying Blockchain technology could further increase transparency by creating tamper-proof records of:

- Contract award decisions and justifications.
- Vendor qualification and evaluation processes.
- Payment authorizations and disbursements.
- Performance evaluation and feedback.

[5] Jakob Svensson, "Eight Questions about Corruption," *Journal of Economic Perspectives* 19, no. 3 (2005): 19-42, https://doi.org/10.1257/089533005774357860.

Mechanisms to increase transparency and boost the probability of detection include: careful and well-developed defence policy and strategy; multi-year planning; cost-effective resources management to build budgets–not least in procurement and personnel decisions–and periodic and *ad-hoc* independent reviews and assessment of the efficiency and effectiveness of defence activities and outcomes. Box 4.2 provides guidance on enhancing the transparency of selected defence activities.

Improving accountability involves strengthening legal/regulatory frameworks. It requires the application of severe sanctions when misconduct is detected. These sanctions must be credible and enforced (i.e. civil and criminal penalties including asset forfeiture, debarment of corrupt contractors from future work, etc.), and publicizing convictions and punishments as a deterrent.

Box 4.3 presents a list of basic measures to enhance integrity, transparency, and accountability in defence.

Box 4.3. Investments to Minimize Corruption

Building Integrity

1. Promote honesty, ethics, and moral values, e.g. through codes of conduct and their effective implementation.
2. Verify compliance with laws, rules, and regulations.
3. Prevent, identify, and reveal conflicts of interest.
4. Introduce screening and selection of personnel.

Increasing Transparency

1. Minimize referral to classified or sensitive information (A culture of secrecy … allows corruption to thrive).
2. Introduce and enhance the capacity for independent audits – for compliance, but also of results and performance.
3. Build the capacity for civilian control by parliament, civil society organizations, and the judiciary as appropriate.
4. Mandate the use of analytical decision tools, such as cost-benefit analysis and professional project management.
5. Introduce policy-/ programme-based budgeting, e.g., by introducing a PPBES (Planning, Programming, Budgeting, and Execution System).

Improving Accountability

1. Provide for timely enforcement of laws, rules, and regulations.
2. Guarantee the independence and professionalism of the judicial system.

Focusing solely on legal sanctions, or on transparency mechanisms is insufficient. The three pillars must work together, and there is no one-size-fits-all recipe. Nations differ in their institutional capacity, culture, history, and risk environment. The optimal mix of integrity/ transparency/ accountability investments depends on the specific characteristics of each country. Coming up with a tailored strategy may also require international cooperation, for example, in sharing intelligence on transnational corruption schemes, coordinating sanctions against corrupt officials, supporting multilateral transparency initiatives, and harmonizing anti-corruption standards across allied nations.

Nation-wide Framework for Democratic Governance

The original strategic approach can be expanded by setting it in a good governance and management framework, nationally and within the defence institution, both in designing and implementing BI programmes. Multiple players beyond a defence ministry can contribute to building integrity efforts. Summarizing the experience of Transparency International's Defence & Security arm, Mark Pyman calls for a 'whole sector' approach embracing companies, regulators, international organizations and civil society organizations to reduce corruption in defence.[6]

The 2010 and this latest edition of the Compendium reflect a more fundamental, nation-wide approach. In established democratic societies, defence ministries and armed forces are subject to rigorous democratic and civilian oversight. A system of checks and balances among the legislative, the executive, and the judiciary branches of power increases the transparency of defence ministries and provides a solid basis for holding officials to account.

Democratic civilian control of the armed forces is key for the transparent and accountable governance of defence. Effective democratic control ensures that armed forces serve the societies that they protect and that they make the best possible use of the resources allocated by elected civilian leadership. These are basic principles and in each country democratic control evolves in a process of their adaptation to specific circumstances.[7]

National parliaments are core players in democratic control. By rigorously debating national defence and security policies, defence expenditures, investment programmes and individual projects, contributions to multinational formations and international operations, and regulating the functioning of the defence ministry and the armed forces by law, the parliament sets the conditions for transparency and accountability. In its oversight function, a parliament is commonly supported by a national audit office. These have the capacity to verify whether allocated resources have been used according to law and in a way that provides best value for money.[8]

The activities of a defence ministry are, just as any other public institution, subject to judicial oversight. Through a legal procedure, courts may examine the lawfulness of a decision-making process and, unless decisions involves classified information, court hearings are open to the public. This form of checks and balances increases the transparency and holds government and public bodies accountable for their actions.

Anti-corruption agencies and specialized prosecutors' offices, whether they are considered part of the judicial system or not, are important players in preventing and revealing cases of corruption and conflicts of interest among public officials.[9] Financial control and internal audit agencies in the executive branch also serve to increase the transparency and accountability of defence ministries and the armed forces.

Since part of the defence activities involve classified information, members of the judiciary and officials of control agencies in the executive that deal with defence matters need to be vetted and allowed access to all relevant documents. Thus, although the respective information cannot be made public, the process of reviewing cases of potential corruption becomes sufficiently transparent and holds defence officials to account.

On the other hand, the perennial question 'Who will guard the guardians?' asked by the Roman poet Juvenal, applies to the members of the judiciary and specialized anti-corruption bodies. The implementation of the strategic approach hangs to a large extent on the proper functioning of oversight and judicial authorities. Its implementation, therefore, needs to take into account the overall health of the oversight institutions and officials, and becomes more challenging during democratic backsliding. The so-called 'third-wave democracies,' including countries in the former Soviet or Yugoslav space, are particularly vulnerable to authoritarian

[6] Mark Pyman, "Tackling Defense Corruption: A "Whole Sector" Approach," in *Ethical Dilemmas in the Global Defense Industry*, ed. Daniel Schoeni and Tobias Vestner (Oxford: Oxford Academic, 2023): 259–304, https://doi.org/10.1093/oso/9780190675813.003.0011.
[7] Simon Lunn, "Ensuring Democratic Control of Armed Forces – The Enduring Challenges," *Connections: The Quarterly Journal* 22, no. 1 (2023): 29-52, https://doi.org/10.11610/Connections.22.1.14.
[8] This and other functions of parliaments are examined in Chapter 12 of this Compendium.
[9] Chapter 13 in this volume examines in detail the role of the anti-corruption agencies.

tendencies. In this process, security institutions and the judiciary may become both tools and victims of backsliding. 'Wannabe' authoritarians aim to dismantle institutions designed to function independently of political interference and replace experts with loyalists.[10]

Members of oversight bodies, specialized anti-corruption agencies, and the judiciary are not immune from prosecution for their actions, or inaction.[11] Recognizing the independence of the judiciary and its crucial role in combating corruption and without prejudice to judicial independence, Article 11 of the United Nations Convention against Corruption calls for measures to strengthen integrity and to prevent opportunities for corruption among members of the judiciary and prosecution services.[12] The Convention explicitly mentions the introduction of codes of conduct as one such measure. Further, the UN Office on Drugs and Crime examines judicial integrity as a comprehensive concept and calls for a broader spectrum of measures for implementing Article 11, 'including in the areas of judicial appointments and careers, case assignment and management systems, judges' outside activities, potential conflicts of interest, communication with the public and media and judicial training.'[13]

Civil society organizations, independent media, investigative journalists and academic institutions support integrity building efforts by raising awareness, policy formulation, capacity building, revealing cases of corruption, and protecting whistle blowers. Such organizations can exercise pressure so that suspected cases of corruption are properly investigated, as well as adopt international norms and good practices. Civil society organizations can also monitor the implementation of anti-corruption strategies and legislation. For all of this, free speech is a fundamental tool.

Civil participation itself should be subject to transparency and accountability. The openness, responsibility, clarity, and accountability of public authorities and civil society organizations, with transparency at all stages of interaction, is an established good practice.[14] Chapter 14 in this volume provides detailed analysis and guidelines for increasing the impact of civil society in BI in defence.

Suppliers of defence products and services, and in particular their associations, can be valuable contributors in setting national and international integrity policies. Leading defence companies provide examples of good practice in setting internal policies for reducing the risks of corruption and conflicts of interest.[15]

The system of checks and balances creates a healthy tension between branches of power and, supported by a vibrant civil society, contributes to initiatives to enhance the integrity of public institutions, including defence. It can be supported by dedicated efforts to strengthen the resilience of our democracies. For example, in her September 2025 State of the Union address, the Commission President Ursula von der Leyen admitted that corruption, capturing independent media, and information manipulation and disinformation all enable democratic backsliding and announced the creation of a European centre for democratic resilience. While at this point details remain unclear, this initiative will bring together expertise and capacity across member states and neighbouring countries and will parallel European anti-corruption and media resilience efforts.[16]

---

[10] Cüneyt Gürer and Elena Walczak, "Democratic Backsliding and Security Governance," *Connections: The Quarterly Journal* 23, no. 4 (2024): 9-31, https://doi.org/10.11610/Connections.23.4.01.

[11] In a recent example, an Italian appeals court upheld a prison sentence for two prosecutors withholding information in a corruption case. See "Italian appeals court upholds conviction for Milan prosecutors in Eni Nigeria case," *Reuters*, October 16, 2025, https://www.reuters.com/business/italian-appeals-court-upholds-conviction-milan-prosecutors-eni-nigeria-case-2025-10-16/.

[12] UN Office on Drugs and Crime, *United Nations Convention against Corruption* (New York: United Nations, 2004), https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

[13] UN Office on Drugs and Crime, "Judicial Integrity," *Thematic Areas in Anti-corruption*, n.d., https://www.unodc.org/corruption/en/learn/thematic-areas/judicial-integrity.html (accessed January 1, 2026).

[14] Conference of INGOs of the Council of Europe, *Code of Good Practice for Civil Participation in the Decision-making Process*, CONF/PLE(2009)CODE1, October 1, 2009, https://www.coe.int/en/web/youth/-/code-of-good-practice-for-civil-participation-in-decision-making-processes.

[15] See, for example, Alice Eldridge and Dominique Lamoureux, "The Defence Industry as an Ally in Reducing Corruption," in *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO & DCAF, 2010), 250-260.

[16] Ursula von der Leyen, "State of the Union 2025," European Commission, September 10, 2025, https://commission.europa.eu/strategy-and-policy/state-union/state-union-2025_en.

The Commission's initiative echoes an earlier call of the NATO Parliamentary Assembly (NPA), recommending in 2019 that the Alliance considers the creation of a Democratic Resiliency Coordination Centre within NATO's institutional structure in order to assist Allies in strengthening their democratic institutions.[17]

Enhancing good governance and professional management in defence establishments can complement national-level efforts to build integrity and reduce corruption in defence.

Competence-Based Checks and Balances within Defence Ministries

The early phases of the BI programme emphasized behaviour in line with legally defined norms and ethical standards. Corresponding measures have been recommended, often in addition to existing organizational processes. Less attention has been paid to actual performance and achieved results, e.g., level of defence capabilities *vis-à-vis* needs and requirements. Therefore, the strategic approach to BI needs to provide consistent, non-contradictory, and feasible frameworks for institutional governance and management that smoothly incorporate counter-corruption and integrity measures. The detailed exploration of such frameworks is beyond the scope of this chapter. Yet, selected good practices in decision-making in resource-intensive processes such as defence procurement are key.

Resource allocation decisions determine how defence budgets are distributed across competing priorities, such as personnel, operations, maintenance, and investment. Internal controls for resource allocation should include standardized cost and performance estimation methodologies, multi-year planning horizons based on realistic assessments of current and future threat environments, and clear and well specified criteria (cost, effectiveness, political and other considerations) for prioritizing competing requirements. Additionally, resource allocation processes should be designed to prevent the concentration of decision-making authority in single individuals or small groups.

Three main decisions in every defence ministry require careful organization:

- *Capability requirements*: Integrating capability needs through transparent prioritization and joint requirements boards limits individual influence, ensuring that decisions are validated by diverse stakeholders.
- *Resource allocation*: Adopting clear budget mechanisms with policy-oriented budgeting, routine budget and performance reviews, internal audits, and cross-checking by independent oversight bodies restricts the opportunity for misuse of funds.
- *Investment projects*: Separation of duties among acquisition managers, contracting officers, and internal auditors establishes structural barriers to collusion and error. Routine reviews, monitoring work plans, and corrective actions should be standard practice.

Decisions in the three respective processes of capability requirements management, acquisition management, and defence resources management are not closed in stovepipes, but are interdependent, balancing needs, solutions, and constraints (Figure 4.2). These three 'pillars' should have separate accountability but coordinated governance. The checks and balances come from:

- Capability requirements drive acquisition;
- Acquisition informs feasibility, affordability, and timelines;
- Resources constrain capability ambitions and necessitate prioritization.

[17] *Resolution 457 on NATO @ 70: Celebrating 70 Years of Peace and Security through Unity*, 184 PC 19 E rev. 1 fin., NATO Parliamentary Assembly, October 14, 2019, https://www.nato-pa.int/document/resolution-457-nato-70.

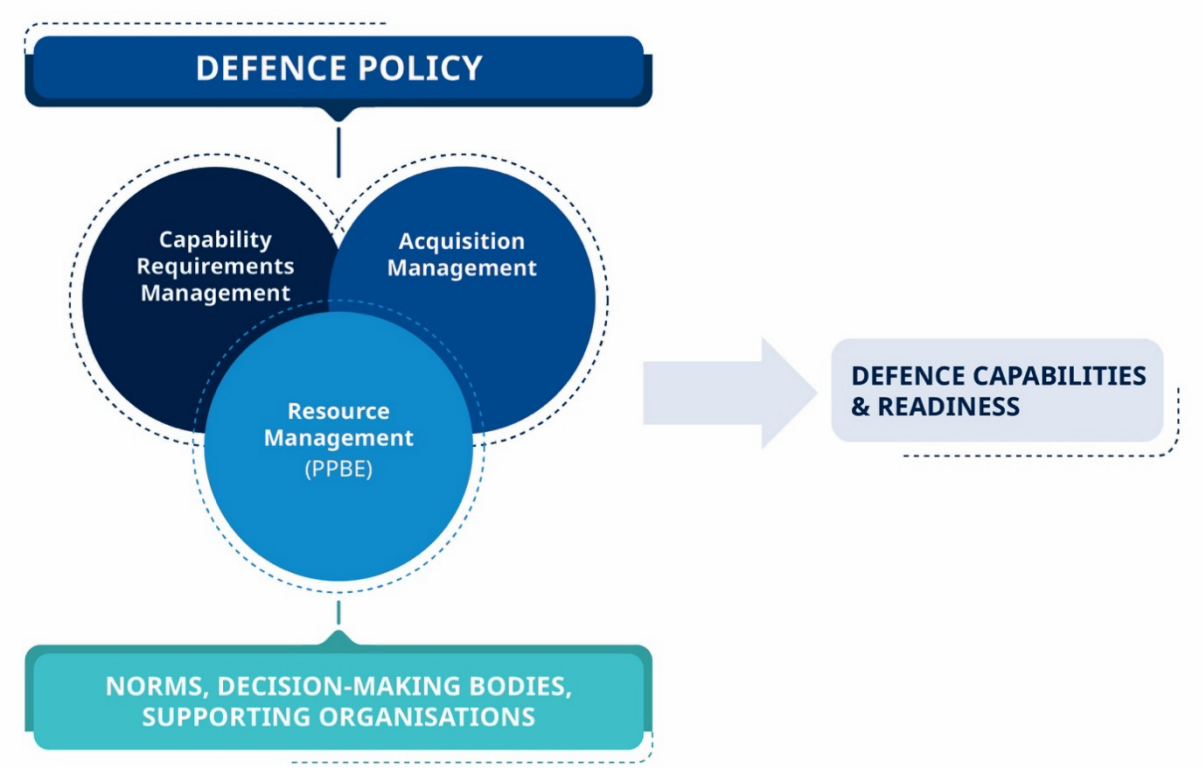


Figure 4.2: Main Defence Management Sub-Systems.

A properly designed governance and management structure allocates decision-making authority to different interacting processes: for capability requirements, acquisition management, and resource allocation. Thus, it provides for an internal system of checks and balances and limits the discretion of individual officials or a specific professional group. Box 4.4 provides an example from Bulgaria.

Many NATO countries implement models with a materiel (procurement) agency as a separate legal entity. In Sweden, for example, the armed forces are responsible for capability planning and maintaining a twelve-year Investment Plan, the Defence Materiel Administration (FMV) is responsible for procurement and logistics, while the Government and then Parliament, on the proposal of the defence ministry, decide on policy and appropriations. Both the armed forces and FMV need to agree before submitting an acquisition project for approval. They have separate reporting lines to the MoD, which ensures mutual oversight rather than subordination.

Ethical behaviour is incompatible with poor results and performance, even if no norms or codes of ethics have been broken. Professionalism in defence management is an irreplaceable ingredient of integrity.

There is an abundance of experience allowing for the identification and codification of good management practices, such as the quality management principles in the international standard ISO 9000. All these principles directly apply to the design and implementation of BI programmes.[18]

[18] For details see Chapter 16 in this volume.

Box 4.4. Checks and Balances in Internal MoD Decision-Making

In the reforms at the end of the 1990s, the Ministry of Defence of the Republic of Bulgaria established a *Programming Council* to review proposed defence and force programmes and to seek a balance in allocating financial resources in view of policy priorities. The corresponding decisions served to guide budget allocations over a six-year horizon and draft the defence budget for the consequent year. This innovation provided for the involvement of all key stakeholders and an impressive increase in the transparency in planning defence expenditures and budget execution.

With the accumulation of experience in the following years, it became clear that debates on the programmes could not reflect all intricacies of the capability needs and requirements and the life cycle of sizeable investment projects. Therefore, amendments to the Law on Defence and Armed Forces in 2009 tasked the defence minister with establishing three different bodies–Programming Council, Defence Capabilities Council, and Armaments Council–and with adopting regulations for their functioning.[19]

The Defence Capabilities Council is chaired by a senior military officer (e.g., Deputy Chief of Defence) and is responsible for reviewing operational needs, defining capability requirements, assessing current capabilities, prioritizing capability needs, and maintaining the information on the overall capability portfolio. In its deliberations, it examines options in meeting capability requirements, but cannot predetermine a specific technological solution or a weapon system that would meet these requirements.

The Armaments Council is chaired by an official responsible for defence investments. It reviews the scope, schedule, cost, performance and risk of a product life cycle to meet approved capability requirements and maintains the portfolio of investment projects.

The Programming Council is chaired by an official with responsibilities for budget planning and execution (currently, the Permanent Secretary of the Ministry of Defence, who is also the ranking civil servant in the MoD). It reviews the programming guidance, submitted defence programmes and budget proposals. It also oversees budget execution and reporting.

The work of the three councils is supported respectively by the Strategic Planning Directorate (J5) in the Defence Staff, the Armaments Policy Directorate, and the Planning, Programming and Budget Directorate of the MoD.

This arrangement brings key stakeholders into decision-making according to their competencies and responsibilities and provides a significant degree of transparency in implementing defence policy.

BI is also a continuous endeavour. It builds on regular reviews of needs and opportunities in cycles to update the understanding of corruption risks,[20] define new goals and objectives, allocate roles, responsibilities and resources, monitor and evaluate results and, potentially, identify the need to amend the BI programme.

The performance of all these tasks can be assisted by advanced technologies. The next and final section of this chapter provides a brief overview of the use of selected technologies in counter-corruption and integrity building efforts.

[19] *Law on Defence and the Armed Forces of the Republic of Bulgaria*, article 33(7), https://lex.bg/laws/ldoc/2135631954. – in Bulgarian.
[20] For examples of good practice see Chapter 15.

Advanced Technologies for Enhancing Integrity in Defence

Advanced technologies can support integrity building in several ways. Digital/ e-procurement or e-tender technologies through a centralized bidding and evaluation platform provide suppliers of defence and related products and services with: an opportunity for easier entry into tenders; more transparent competition; and a digital audit trail. The use of such platforms reduces favouritism and strengthens public oversight.

Most NATO and many partner countries use e-procurement platforms. For example, the United Kingdom's Ministry of Defence uses the Defence Sourcing Portal (DSP), where all MoD advertised requirements are published, creating a single, auditable channel for competitions and supplier notifications. In France, Romania, and Bulgaria it is mandatory to use the e-tender platform of the central government for non-classified purchases. This enhances competition and transparency with full electronic trails of procedures, including time-stamping.

The mandatory use of such platforms allows for the implementation of cyber forensics tools for recovery of digital evidence, verification, forensic audits, and supporting legal prosecution.

Data analytics employing machine learning, other types of artificial intelligence or 'traditional' decision support methods can be employed to predict or detect fraud. An example is detecting patterns indicative of irregular bidding, collusion, or other types of conflicts of interest. Data analytics enable early anomaly detection of cases with higher corruption risks and can be used to direct oversight. Big data integration is a particular class of data analytics, enabling cross-checks of personnel, logistics, and financial data and allowing for the prevention of duplicate contracts and hidden budget leakage.

Blockchain and distributed ledger technologies allow immutable contract and asset verification. They provide tamper-proof records and can expose phantom deliveries.

Finally, digital ID and biometrics tools serve to verify personnel authenticity and payroll integrity. They can contribute to eliminating ghost soldiers and payroll fraud.

The successful integration of these technologies demonstrates that anti-corruption in defence depends not only on policy but also on innovation. Countries that combine multiple systems–e.g., e-procurement linked to financial databases–create end-to-end transparency. Emerging economies have also shown that even modest investments in technology yield measurable integrity gains.

Advanced technologies support integrity building by enabling public scrutiny and reporting on corruption, enhancing transparency and accountability, facilitating citizen participation and government-citizen interactions. Of course, they also allow new opportunities for corruption and avoiding detection using the dark web, cryptocurrencies, or cyber manipulation of centralized databases. The introduction of technological tools does not bring results automatically. It is not only the misuse/abuse of technological tools by malign actors that should be considered a risk factor. These technologies come with some flaws of their own (at least in their current stage of development), including vulnerability to cyberattacks and hacking, and in the particular case of AI, deviations such as hallucinations and sycophancy. Finally, their impact depends on adapting the technological tools and the local context, including investments in requisite skills and technological capacity.[21]

Conclusion

The ongoing war launched by Russia against Ukraine is by far the largest war in Europe since the end of the Second World War. It changed the threat perceptions of NATO members and partners, leading to a significant increase in defence budgets and efforts to meet urgent capability requirements in ever shorter innovation timescales. In this environment, even a few cases of corruption in defence may lead to reduced political and public support and, subsequently, insufficient investments in deterring and defending against a potential

[21] Isabelle Adam and Mihály Fazekas, "Are emerging technologies helping win the fight against corruption? A review of the state of evidence," *Information Economics and Policy* 57 (2021), 100950, https://doi.org/10.1016/j.infoecopol.2021.100950.

aggressor. Therefore, counter-corruption efforts will remain close to the top of the agenda of policy-makers and societal watchdogs.

The 2010 Compendium proposed a strategic approach to reducing corruption in defence by investing in integrity, transparency, and accountability. This approach has proved its value. This chapter extends it by stressing the importance of having in place national and intra-institutional frameworks of checks and balances and opportunities provided by merging technologies to support counter-corruption efforts.

The following chapters provide details on corruption challenges in functional areas of defence. They also outline good practices that can inform the design and assist the implementation of building integrity programmes of national defence ministries, armed forces, and other security institution

5. The Evolution of NATO's Strategic Approach to Integrity and Good Governance in the Defence and Related Security Sector

Dr. Nadja Milanova

Introduction

The NATO Strategic Concept of 2022 highlights the importance of good governance as being essential for the implementation of the three core security tasks of the Alliance: defence and deterrence; crisis prevention and management; and cooperative security.[1] Furthermore, the Strategic Concept underscores the role of weak governance in perpetuating terrorism.[2] These high-level statements have demonstrated NATO's steadfast and continued commitment to values, democracy and the rule of law as enshrined in the North Atlantic Treaty.[3] In a volatile security context, the protection of democratic values remains more pertinent and relevant than ever. Even more, the shifting strategic environment has sharpened the focus on the significance of good governance as a security enabler. NATO has acknowledged that a lack of good governance and its derivatives, not least corruption, is a security threat that has a negative impact on peace and stability. NATO's strategic approach to building integrity and strengthening good governance in the defence and related security sector has become, meanwhile, part of the security paradigm.

The reference to good governance in the 2022 Strategic Concept, for the first time in such a document, is a culmination of the NATO Building Integrity (BI) Initiative, referred to as NATO BI. Through NATO BI the Alliance has mainstreamed its strategic approach to strengthening good governance in the defence and related security sector since 2007. At the same time, highlighting the importance of good governance at the highest strategic level has opened the debate on the need to rethink methodologies and tools, and consequently expand the scope of NATO's approach to the constituting elements of security sector governance as a more holistic concept. NATO's potential future role in a broader security sector governance framework is still to be conceptualized, defined and formalized. However, any forward-looking perspective to this end will draw upon the outcomes, challenges and lessons learned from the systematic efforts undertaken by the Alliance to place the corruption-security nexus on the security agenda, and to promote integrity, transparency and accountability as a countermeasure to potential mismanagement of defence resources and possible corruption risks in defence.

The NATO BI Initiative was established in 2007 by NATO's Euro-Atlantic Partnership Council (EAPC) as a capacity-building programme. It was aimed at supporting the development of transparent and accountable defence institutions in response to the growing concern about the risk of corruption in the defence and related security sector.

The establishment and subsequent expansion of the NATO BI Initiative into a full-fledged programme with a long-term perspective is due to the unwavering support of several NATO countries that ensured adequate resources with financial contributions to the NATO BI Trust Fund,[4] later transformed into the BI Initiative of the NATO Partnership Trust Fund, and in-kind contributions with expertise and knowledge transfer. The BI Steering Group, and later the BI Advisory Group (BIAG),[5] have provided strategic guidance and political support. In addition, NATO BI continuously looked for synergies and complementarities within the growing BI Community of Practice, including international organizations, national institutions, academia, civil society, and the private sector, in

[1] NATO, *NATO 2022 Strategic Concept*, adopted by Heads of State and Government at the NATO Summit in Madrid, June 29, 2022, last updated March 3, 2023, https://www.nato.int/cps/en/natohq/topics_210907.htm.
[2] Ibid., para. 10
[3] NATO, "The North Atlantic Treaty," April 4, 1949. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.
[4] The BI Programme developed in stages with clearly defined implementation objectives, with the support of committed NATO and partner countries at each stage.
[5] As of 2025, the members of the BI Advisory Group are Norway, United Kingdom and Switzerland.

particular the International Forum on Business Ethical Conduct (IFBEC). In line with NATO's comprehensive approach,[6] the importance of good governance in the defence and related security sector and the recognition of NATO's expertise in this area became prominent in NATO's dialogue with other international organizations, namely the European Union, the United Nations Office on Drugs and Crime (UNODC), and the UN Department of Peace Operations (UNDPO). Following the signing of an agreement in December 2018, NATO and the EU launched their cooperation in the area of BI and cooperation on BI and good governance in the defence and related security sector.[7] The BI Trust Fund members and the European Commission signed an agreement for BI and good governance cooperation, entailing an EU financial contribution to NATO BI Trust Fund for the period of 2019-2023. This included EU participation in the BI Steering Group and later the BI Advisory Group; peer-to-peer exchanges; and participation with expertise in BI capacity building in beneficiary partner countries.

With robust political support, the 2010 DCAF publication on *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices*[8] has, in large part, provided the intellectual drive for the evolution of NATO's approach to BI. The publication set out a list of recommendations for institutionalizing a strategic approach to reduce corruption through:

- Strengthening good governance with a special focus on integrity, transparency and accountability;
- Incentivizing a change of behaviour among defence officials by reducing perceived rewards of corrupt behaviour and increasing the expected costs;
- Implementing a multi-year programmatic approach to BI initiatives;
- Increasing transparency and improving accountability as a way to minimize corruption risks, while ensuring efficient defence spending;
- Conducting regular assessments of institutional capabilities and responses to corruption.[9]

BI means countering weak governance and corruption risks versus the 'eradication of corruption', another distinct approach that has gained traction in the academic research and in policy making in recent years. As posited by researchers, 'integrity building or good governance' as a preventive mechanism versus 'counter-corruption' or 'corruption eradication' that are two different paradigms for addressing corruption risks.[10] It is acknowledged that the first, preventive approach is subtler as 'it admits that good governance cannot be "restored" but needs more complex "building"'.[11] This also broadens the parameters of building integrity, which is often thought of as solely an anti-corruption concept due to the tendency to narrow the scope and limit the narrative. Yes, preventing corruption and minimizing corruption risks in defence lies at the core of NATO's BI Initiative. However, the desired outcomes and the pathways to achieve them are more than just implementing anti-corruption strategies *per se,* but rather they are about instilling the principles of integrity, transparency and accountability as a prerequisite for ensuring the effectiveness and efficiency of defence institutions.

NATO's Strategic Approach to Integrity and Good Governance

With the establishment of its BI initiative, NATO has embraced the rationale of addressing the risk of corruption in the defence and related security sector in a preventive manner. NATO BI works through the prism of governance norm setting, institution building, and defence resource management. Assuming the political nature of defence reforms and transformation taking place in a specific governance context, NATO has gradually and

---

[6] NATO, "A 'Comprehensive Approach' to Crises," last updated March 7, 2024, *NATO — Partnerships and Cooperation*, https://www.nato.int/en/what-we-do/partnerships-and-cooperation/a-comprehensive-approach-to-crises (accessed February 23, 2026).
[7] See at NATO, "Norway, Switzerland, the UK and EU Sign Building Integrity Arrangement for 2019–2022 with NATO," December 18, 2018, https://www.nato.int/en/news-and-events/articles/news/2018/12/18/norway-switzerland-the-uk-and-eu-sign-building-integrity-arrangement-for-2019-2022-with-nato (accessed February 23, 2026).
[8] *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO & DCAF, 2010), https://www.nato.int/cps/en/natohq/topics_104893.htm.
[9] Chapter 2, "A Strategic Approach to Building Integrity and Reducing Corruption in Defence," in *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO & DCAF, 2010), p. 8.
[10] Alina Mungiu-Pippidi, *The Quest for Good Governance: How Societies Develop Control of Corruption* (Cambridge: Cambridge University Press, 2015), p. 10.
[11] Ibid. p.10.

incrementally developed a strategic framework for addressing corruption and weak governance risks in the defence and related security sector. This strategic framework comprises:

- Understanding of corruption and weak governance and its impact as a security threat;
- Strategic level guidance for building integrity, increasing transparency and improving accountability as a strategic priority for Allies, partners and NATO;
- Systematic approach to mainstreaming the principles of integrity, transparency and accountability through NATO policies and procedures;
- Holistic approach to defence reforms and transformation through a multiyear programmatic lens; and
- Multistakeholder collaboration.

Understanding the Corruption-Security Nexus

At the NATO Warsaw Summit in 2016, Heads of State and Government stated that corruption and poor governance are security challenges that undermine democracy, the rule of law and economic development.[12] The corruption-security nexus is the underlying premise of the NATO BI Policy endorsed by Heads of State and Government in Warsaw.[13] There it was pronounced that 'corruption and poor governance are security challenges as they undermine democracy, the rule of law and economic development, erode public trust in defence institutions and have a negative impact on operational effectiveness'.[14] At the Brussels Summit in 2021, NATO reiterated that '[c]orruption and poor governance undermine democracy, the rule of law, and economic development, thus constituting challenges to our security'.[15]

NATO's high-level statements on the corruption-security nexus are corroborated by the World Economic Forum analysis of global risks, whereby governance falls into geopolitical group risks.[16] At the Warsaw Summit in 2016, NATO defined resilience as the full spectrum of threats and agreed on seven baseline requirements for national resilience against which member states can measure their level of preparedness. These include assured continuity of government and critical government services; resilient energy supplies; ability to deal effectively with people's uncontrolled movement; resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems; and resilient civil transportation systems.[17] In 2021, the NATO Brussels Summit adopted the Strengthened Resilience Commitment, which *inter alia* acknowledges the diverse challenges to resilience, including attempts to undermine the Alliance's shared values and interference with democratic processes and good governance.[18]

According to the Organisation for Economic Co-operation and Development (OECD), corruption is identified as the number one concern for citizens.[19] Estimates show that the global cost of corruption equals more than 5% of global GDP (USD 2.6 trillion according to the World Economic Forum) with over USD 1 trillion paid in bribes

[12] NATO, "Warsaw Summit Communiqué," NATO, July 9, 2016, para. 130, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[13] NATO, "NATO Building Integrity Policy," July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_135626.htm?selectedLocale=en#:~:text=The%20NATO%20Building%20Integrity%20Programme%20is%20part%20of,terms%2C%20integrity%20is%20directly%20linked%20to%20good%20governance.
[14] Ibid, para. 2.
[15] NATO, "Brussels Summit Communiqué," June 14, 2021, para. 62, https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.
[16] World Economic Forum, *The Global Risks Report 2020* (Geneva: World Economic Forum, January 15, 2020), https://www.weforum.org/reports/the-global-risks-report-2020.
[17] NATO, "Commitment to Enhance Resilience Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw, 8-9 July 2016," July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133180.htm (accessed February 23, 2026).
[18] NATO, "Strengthened Resilience Commitment," June 14, 2021, para. 7, https://www.nato.int/cps/en/natohq/official_texts_185340.htm?selectedLocale=en (accessed February 23, 2026).
[19] Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Public Integrity*, January 26, 2017. OECD is encouraging a sector-based approach to public integrity.

each year, according to the World Bank.[20] The Association of Certified Fraud Investigators (ACFE) analyses cases of fraud, corruption included, across different industries and regions. In its annual Report to the Nations for 2018, the ACFE concluded that occupational fraud remains an enormous threat to the global economy.[21]

The OECD reports that on average corruption decreases investment by 5% and increases the cost of doing business by 10%.[22] All sectors are vulnerable. Analysing cases of the bribery of foreign public officials, OECD ranks the extractive, construction, transportation and storage, and information and communication sectors as the leading four sectors where corruption operates. Public administration and the defence sector are ranked in ninth position. The OECD estimates that the total amount of bribes paid in public administration and defence, relative to the transaction value by sector, is 8 %, i.e. this is the relative 'cost' of bribes for the sector.[23] This can be indicative of the scope of concerns related to the defence sector, in light of the recently published defence expenditures for the NATO countries in the period of 2014–2025.[24]

The establishment of NATO BI as a distinct strand of work has acted as a catalyst for raising awareness about potential corruption risks in defence as a security threat and the remedial impact of strengthening integrity and governance as a prevention measure. Safeguarding defence expenditures remains a priority. However, from a risk assessment and risk management perspective, the resilience of the defence sector against mismanagement and waste of resources also defines the sustainability of defence capabilities. With intellectual input by civil society[25] NATO BI has shaped the debate on integrity and good governance by identifying defence-sector corruption risks and grouping them into categories that underpin the analysis of defence institutions and that inform missions and operations. Its aim is to raise awareness, deepen understanding of how corruption undermines defence capabilities, operational effectiveness and mission success, and foster leadership commitment to BI.

Strategic Level Guidance and Mainstreaming Integrity Building

NATO's work on BI has gained institutional traction thanks to the consensus among Allies on the importance of this line of effort – both on the political and military side – and the strategic guidance provided over the years towards completing the overall framework of political statements and policy documents needed to operationalize the concept. The NATO BI Policy, endorsed by the NATO Heads of State and Government in 2016, set out the strategic direction for this work, reaffirming that:

- BI is a key element of Alliance activities;
- The importance of implementing measures to improve integrity building, anti-corruption and good governance applies to NATO as an organization, and Allies and partners alike;
- Effective and transparent national procedures need to be in place to assess corruption-related security risks and defence requirements, and to develop and maintain efficient and interoperable defence capabilities corresponding to these requirements and international commitments;

[20] United Nations , "Global Cost of Corruption at Least 5 Per Cent of World Gross Domestic Product, Secretary-General Tells Security Council, Citing World Economic Forum Data," September 10, 2018, https://www.un.org/press/en/2018/sc13493.doc.htm (accessed February 23, 2026).
[21] Association of Certified Fraud Examiners, *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse* (Association of Certified Fraud Examiners, 2018).
[22] Organisation for Economic Co-operation and Development (OECD), *OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials* (Paris: Organisation of Economic Co-operation and Development, 2014).
[23] *Ibid.,* pp. 27. OECD points to a surprising variation between the sectors, e.g. bribes in the water supplies and education sectors each amounting to 2% of the transaction value compared to the extractive and wholesale/retail trade sectors, where bribes amounted to respectively 21% and 19% of the transaction value.
[24] NATO, "Defence expenditure of NATO Countries (2014-2025)," August 28, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/08/28/defence-expenditure-of-nato-countries-2014-2025.
[25] Mark Pyman, *Building integrity and countering corruption in defence and security: 20 practical reforms* (Transparency International Defence & Security, 2011), p. 10, https://curbingcorruption.com/wp-content/uploads/2018/07/Pyman-2011-Building-integrity-and-countering-corruption-in-defence-and-security-20-practical-reforms.pdf.

- BI should be an integral part of NATO work and activities internally and that all NATO civilian and military structures should continue to make efforts in BI, transparency and accountability and promote good governance within their structures.[26]

Furthermore, in the aftermath of the Warsaw Summit, Heads of State and Government reaffirmed at the Brussels Summits of 2018 and 2021, their conviction that transparent and accountable defence institutions under democratic control are fundamental to stability and essential for international security cooperation. In 2021, Heads of State and Government reiterated that 'implementing measures to improve integrity building, to fight against corruption, and to foster good governance is of continued importance for NATO, Allies, and partners alike'.[27]

The BI Policy stipulated the need for integrity building to be incorporated in the fulfilment of NATO's core tasks, setting out its rationale for this:

- Collective defence depends on effective and efficient defence institutions based on the principles of integrity, transparency and accountability, maximizing the value of money to further build defence capabilities and ensuring better resourced Armed Forces;
- Crisis prevention whereby BI plays a preventive role that also needs to be considered in all stages of NATO-led operations and missions; and
- Cooperative security that requires the implementation of integrity principles, sharing of lessons learned and good practices, within and across the various partnership formats.[28]

The implementation of the BI Policy has been supported by a BI Action Plan with two iterations so far, for the period of 2016–2020 and 2021–2025, both noted by NATO Foreign Ministers at their meeting in December 2016 and by NATO Defence Ministers in February 2021. All relevant documents and statements have therefore provided strategic guidance for a structured approach to operationalizing BI and good governance along NATO's political and military lines of activity through civil-military cooperation across the strategic, operational and tactical levels.

The strategic guidance directs the mainstreaming of integrity building into NATO policies and procedures. Several examples point to this:

- Building Integrity was introduced for the first time as a separate domain in the NATO Defence Planning Capability Survey for member states in 2017; since then, a chapter with BI-related questions has been systematically included in the survey, highlighting the importance of this area of work for maximizing the value for defence capabilities and ensuring better-resourced Armed Forces and resilient institutions. A number of Allies have reflected the impact of corruption on stability and on operational effectiveness in their national security strategies and defence reviews, such as the U.S. National Security Strategy (2022),[29] the Norwegian Armed Forces' Joint Operational Doctrine,[30] the Netherlands Integrated International Security Strategy 2018-2022; while the 2025 Strategic Defence Review of the United Kingdom[31] highlights the importance of leadership, human resources management, skills and adaptive learning, which are constituent elements of NATO's approach to BI with regard to the effective and efficient management of resources;

[26] NATO 2022 Strategic Concept.
[27] "Brussels Summit Communiqué," Para. 62.
[28] Ibid.
[29] The White House, *National Security Strategy* (October 2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[30] Norwegian Armed Forces, *Forsvarets fellesoperative doktrine 2019 [Joint Operational Doctrine 2019]* (Oslo: Norwegian Armed Forces, 2019).
[31] UK Ministry of Defence, *The Strategic Defence Review 2025 - Making Britain Safer: secure at home, strong abroad* (2025), https://assets.publishing.service.gov.uk/media/683d89f181deb72cce2680a5/The_Strategic_Defence_Review_2025_-_Making_Britain_Safer_-_secure_at_home__strong_abroad.pdf.

- BI has been mainstreamed into NATO partnership mechanisms as a way to ensure the sustainability and continuity of integrity-related reforms in defence establishments of partner countries; since 2014, most of the countries have included a partnership goal on integrity development in their Partnership Planning and Review Process (PARP); for some countries, integrity has been successfully incorporated as a cross-cutting issue in other partnership goals, such as personnel management and defence planning. This has enabled the process of aligning BI with the transformation and modernization of Ministries of Defence and Armed Forces of partner countries;
- BI is integrated as a strategic priority and implementation goal in the Individually Tailored Partnership Programmes (ITPPs) for most of the partners;
- BI is also a component of the Defence Capacity Building (DCB) Initiative since its establishment at the Wales Summit in 2014 and is an integral part of the existing NATO DCB Packages for five partner countries[32], making integrity and good governance a part of the political engagement and dialogue with partners and part of the process of improving partners' interoperability and building their operational capacity;
- BI is also implemented in relation to other NATO policies and concepts, such as gender/women, peace and security, small arms and light weapons (SALW), counter-terrorism, stability policing, security force assistance, in coordination with other international community stakeholders with a comprehensive approach mindset.

On the military side, the Military Concept for BI in Operations (BIIO) adopted in February 2021 finalizes the architecture of documents needed to make BI operationally applicable across NATO's political and military lines. Further to this, the impact of corruption and the need to focus on BI development is reflected in several NATO doctrines. For example, the Allied Joint Doctrine (AJP-01) dated December 2022 takes corruption and poor governance as factors of the strategic context and points to BI as a key element of Alliance activities.[33] The Allied Joint Doctrines for Stability Policing (AJP-3.22),[34] for Military Support to Stabilization and Reconstruction (AJP-3.4.5),[35] and for Security Force Assistance (AJP-3.16)[36] are also examples of NATO military documents taking the BI Policy into account and prescribing integrity building measures at the operational and tactical levels.[37]

Operationalizing Integrity and Good Governance

The overarching aim of the NATO BI Policy is the development of 'effective, transparent and accountable defence institutions which are responsive to unpredictable security challenges, including those of a hybrid nature'.[38] The drafting of the policy had built upon the experience gained through the implementation of NATO BI since 2007 in both NATO and partner countries. This experience led to the NATO definition of integrity as being 'the link between behaviour and principles.' It is further elaborated that this requires the institutionalization of integrity standards within defence or related security establishments, and the socialization of institutional norms and values among their personnel.[39] Therefore, in essence, NATO's approach to BI in the defence and related security

[32] Bosnia and Herzegovina, Iraq, Jordan, Republic of Moldova, and Tunisia.
[33] NATO Standardization Office*, Allied Joint Doctrine (AJP-01)* (December 2022), https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf.
[34] NATO Standardization Office , *Allied Joint Doctrine for Stability Policing (AJP-3.22)* (July 2016), https://assets.publishing.service.gov.uk/media/5a821ac2ed915d74e3401bfe/20160801-nato_stab_pol_ajp_3_22_a_secured.pdf.
[35] NATO Standardization Office, *Allied Joint Doctrine for Stability Policing (AJP-3.22)*, Edition A Version 1, promulgated July 14, 2016, https://assets.publishing.service.gov.uk/media/667d6a6d4ae39c5e45fe4d4c/ARCHIVE-AJP_3_4_5_stabilization_2015.pdf#:~:text=AJP-3.4.5%20is%20intended%20for%20use%20primarily%20by%20joint,provides%20guidance%20on%20the%20conduct%20of%20joint%20operations.
[36] NATO Standardization Office & Ministry of Defence, *Allied Joint Doctrine for Security Force Assistance (AJP-3.16),* Edition B Version 1, published August 14, 2017, updated September 3, 2025, https://www.gov.uk/government/publications/allied-joint-doctrine-for-security-force-assistance-sfa-ajp-316a.
[37] Ludovica Glorioso (ed.), *Promoting the Rule of Law and Good Governance: SFA Implications in International Initiatives* (Rome: NATO Security Force Assistance Centre of Excellence, 2021), https://www.nsfacoe.org/wp-content/uploads/2021/09/Promoting-the-Rule-of-Law-and-Good-Governance.-SFA-Implications-in-International-Initiatives..pdf.
[38] NATO BI Policy, para. 6.
[39] NATO BI Policy, para. 3.

sector consists in defining integrity standards, embedding them at an institutional level through policies and procedures, and developing an organizational culture and mindset.

Integrity Standards

The UN Convention against Corruption (UNCAC) spells out the governance norms in the prevention and control of corruption. Article 1 (promotion of integrity and accountability), article 7 (public sector) and article 9 (procurement) are most relevant for NATO. Those provisions are transposed, to a large extent and with elements critical to the defence sector, into the Partnership Action Plan for Defence Institution Building (PAP-DIB),[40] adopted at the NATO Istanbul Summit in 2004. PAP-DIB defines NATO's principles that are considered fundamental to the development of effective and democratically responsible defence institutions. The main BI-related focus is on the democratic control of defence activities; on the effective and efficient measures to optimize the management of defence institutions and defence resources, including personnel; financial planning and resource allocation; and on defence spending in a transparent and viable manner.
The principles listed in PAP-DIB represent the overall set of integrity standards that NATO seeks to embed in the defence and related security sector.[41] With its establishment and evolution over time, NATO has provided practical solutions in this regard, first and foremost through the BI Self-Assessment and Peer Review Process, known as the NATO BI Process (see Box 5.1.)

Embedding Integrity Standards: The institutional Level

The BI Process is the main NATO tool for identifying institutional vulnerabilities and for proposing recommendations for further reforms to participating countries, be they NATO countries or partners. The integrity standards as encoded in the PAP-DIB form the basis of the BI Self-Assessment Questionnaire,[42] in conjunction with the identified areas of corruption risks in defence. Both Allies and partners can opt for the completion of the questionnaire as an entry-level commitment for undergoing NATO assessment and peer review. The two-phased process provides a baseline analysis of national practices and procedures, identifies good practices, and offers recommendations for further improvement.

Box 5.1. NATO BI Self-Assessment and Peer Review (NATO BI Process)

Goals of the NATO BI Process

1. Support countries/participating institutions to assess their integrity systems, identify gaps and needs for further improvement, and highlight good practices;
2. Enable the provision of assistance through capacity building and advisory services in line with identified needs and gaps;
3. Promote and facilitate the exchange of national experiences and good practices;
4. Strengthen international cooperation on good governance in the defence and related security sector.

Guiding principles of the NATO BI Process

5. Voluntary, upon demand;
6. National ownership and commitment;
7. Positive, non-intrusive, non-adversarial, and non-ranking;
8. Transparent, integrated, impartial and constructive;
9. Trust and cooperation.

[40] NATO, "Partnership Action Plan on Defence Institution Building (PAP-DIB)," May 16, 2025, https://www.nato.int/cps/en/natohq/topics_50083.htm (accessed February 23, 2026).
[41] The defence sector is the primary stakeholder for NATO. Over the years, following on the engagement of their defence ministries with NATO on BI, several countries have extended BI to their related security institutions, e.g. in 2019 BI Process for Ukraine covers nine institutions of the whole defence and security sector.
[42] The NATO BI Self-Assessment Questionnaire comprises eight chapters and allows elaboration on nation-specific questions, if relevant.

Stages of implementation

10. Self-initiated completion of the Self-Assessment Questionnaire by the participating country/institution;
11. Launch of the peer review by NATO upon receiving the completed questionnaire;
12. Conduct of in-country consultations led by NATO with a team of experts;
13. Submission of NATO's final report with recommendations for further action.

Enabling factors at a national level

14. High-level political commitment;
15. Leadership support and guidance;
16. Middle-management support and engagement;
17. Coordination mechanism to integrate the institutional knowledge of policies and procedures from across different functional areas;
18. Change management culture at an institutional level.

Expected results

19. Drives sustained reforms and provides momentum towards a stronger integrity framework;
20. Enhances transparency and mobilizes national commitment;
21. Provides a platform for knowledge transfer, expert dialogue and exchange of lessons learned;
22. Develops national capabilities for risk assessment and design of integrity strategies and mitigation measures, including legislative and policy amendments, institutional reforms, and enhanced national coordination;
23. Strengthens international cooperation in the area of integrity and good governance in the defence and related security sector.

As of 2025, 21 countries – both allies and partners – have completed or are in the process of completing the BI Self-Assessment and Peer Review Process, some of them two or more times. These are: Afghanistan (2011), Armenia (ongoing), Bosnia and Herzegovina (2014), Bulgaria (2010), Colombia (2016; 2023), Croatia (2014), Georgia (2013; second time ongoing); Hungary (2015), Iraq (2023), Jordan (ongoing), Latvia (2013), the Republic of Moldova (2016; 2024), Montenegro (2016; questionnaire completed for the second time in 2022); the Republic of North Macedonia (2015); Norway (2010); Peru (ongoing), Poland (2016), Serbia (2012), Tunisia (2024), Ukraine (2010; 2013; 2017; and 2019), and the United Kingdom (2019 peer review visit).[43]

The BI Process relies on the expertise of experts from Ministries of Defence, notably Norway and the United Kingdom, as well as independent experts as part of the NATO-led in-country consultations, analysis of the replies to the questionnaire, report drafting, and design of recommendations. In essence, the BI process encapsulates the collective international knowledge on integrity in the defence sector developed over the last twenty years. The BI Process is not an end in itself; it is a means of:

- Generating a national strategic-level political commitment to integrity building and strengthening good governance in defence and security;
- Forging national ownership and buy-in so that national institutions voluntarily choose to complete the BI questionnaire (the usual entry point to a NATO assessment), often after two to three years of active engagement with NATO;
- Sustaining the national commitment to integrity and good governance reforms after the submission of the NATO final report with recommendations;
- Developing knowledge of the system's vulnerabilities and mitigating measures; the completion of the questionnaire and the in-country peer review consultations are setting defence institutions on a learning trajectory;

[43] In December 2012, NATO launched a BI Tailored Programme for South Eastern Europe (SEE) following the approval of a BI Project by the South Eastern Defence Ministerial Process (SEDM) at its meeting in Sarajevo in October 2012 during the chairmanship of Bulgaria.

- Instilling a long-term, multi-year perspective to good governance reforms; the conduct of the BI Process builds capacity and prepares defence leaders and officials to proceed with reforms based on NATO recommendations complementary to national strategies and obligations in the implementation of international anti-corruption provisions.

The BI Process factors in the country-specific context in terms of the political and governance framework in place as well as the level of maturity of each country with regard to integrity initiatives and the implementation of the principles of transparency and accountability. NATO has acted like 'an external agency influence'[44] for reforms not by transferring institutional models but by generating momentum and incentivizing integrity reforms through positive engagement with national authorities in an area of critical sensitivity. The premise of the BI Process as a diagnostic and capacity-building tool is that promoting integrity standards is 'largely a political rather than a technical-legal process'.[45] The NATO BI country-specific strategies are anchored in the respective stages of implementation of the BI Process, i.e. development of integrity plans, implementation of the peer review report recommendations, or capacity building in functional areas, and establishment of expertise in functional areas in accordance with countries' identified needs and gaps, such as *inter alia* the multi-year programme for strengthening the internal audit function of the Ministry of Defence of Georgia organized by NATO with the support of an international audit expert; NATO's support to the development of the Code of Conduct of Ukraine's Ministry of Internal Affairs; and the conduct of the accountability analysis and recommendations as part of NATO's Strategic Defence Procurement Review (SDPR) for Ukraine in 2024, contributing to the implementation of Ukraine's Interoperability Roadmap and the Annual National Programme (ANP) for reforms.

At the stage of implementation, partner countries and their defence and related security national institutions benefit from the expansive expertise on BI and good governance of several organizations. Among these are, most notably: the Centre of Integrity in the Defence Sector (CIDS) of the Ministry of Defence of Norway, the Geneva Centre for Security Sector Governance (DCAF), the UK Defence Academy, the UK TI-DS, Romania's Regional Department of Defense Resources Management Studies (DRESMARA), and the Central Organisation Integrity Defence (COID) of the Dutch Ministry of Defence. These organizations, among others, have ensured that BI grows steadily into a distinct field of research and practice. They have supported NATO in enhancing its knowledge base by designing tools and methodologies, and by developing transferrable knowledge materials based on good practices and lessons learned, especially with regard to the institutional functional areas relevant to BI. Examples might include: corruption risk assessment; human resources management; code of conduct, ethics and leadership; internal audits; procurement; and relations with the defence industries.

The impact of countries' engagement with the NATO BI process and its follow-up is measured by several metrics. These include the sustainability of political commitment over a multi-year framework, the incremental improvement of institutional policies and procedures to mitigate identified gaps and vulnerabilities, and the robustness of institutions best tested in times of political and security uncertainty, not least electoral cycles. The idea of the cyclical nature of implementation through all the steps of the BI process is captured in Figure 5.1.

[44] Mungiu-Pippidi, *Quest*, p. 186.
[45] Mungiu-Pippidi, *Quest*, p. 209.

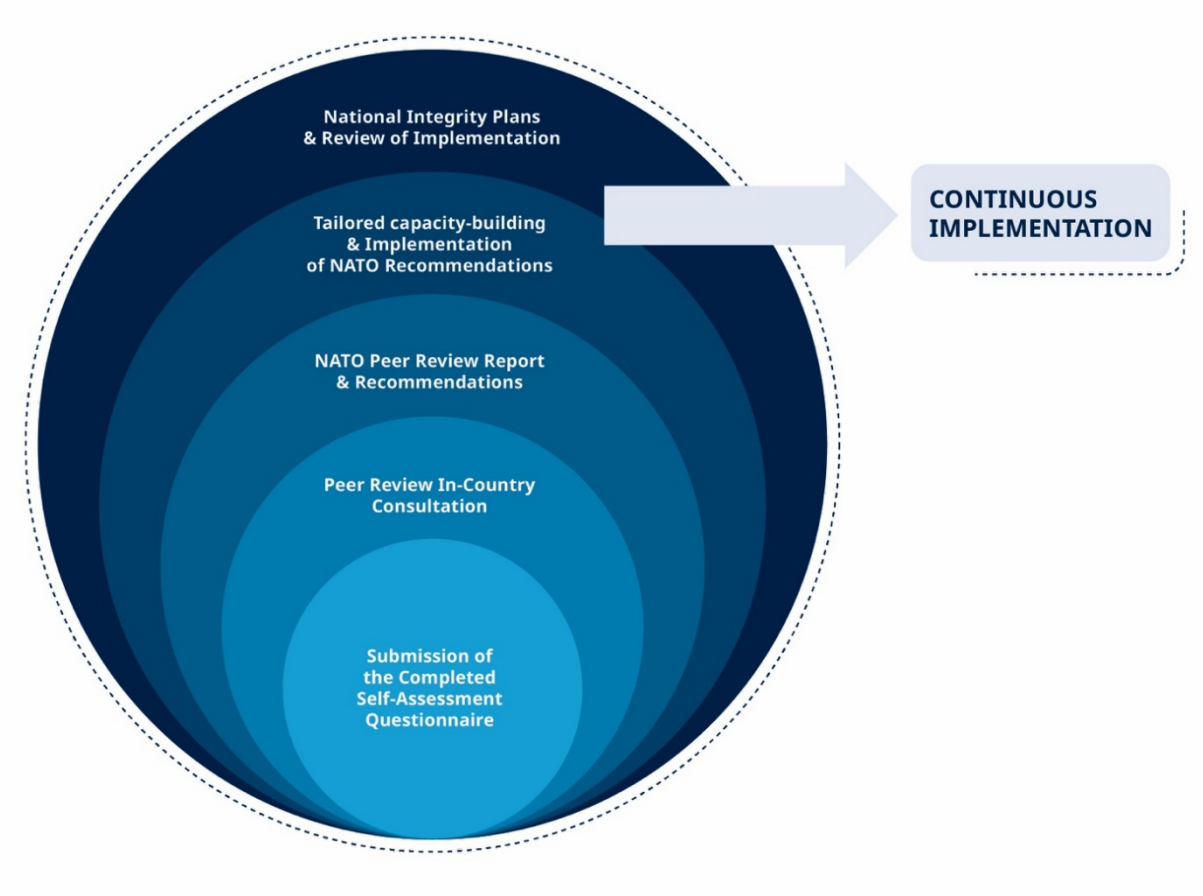


Figure 5.1: Implementation Cycle of the NATO BI Self-Assessment and Peer Review Process.

The main criteria for assessing integrity building reforms are national integrity action plans and a mechanism to review implementation; the level of transparency in decision-making across the different functional areas of defence institutions, e.g. merit-based recruitment and promotion, competitive procurement, etc.; the level of accountability in planning, budgeting and defence resources management; the level of independence and objectivity of oversight and scrutiny. While the non-linear nature of reforms is acknowledged, the assessment of progress needs to be based on evidence in light of identified gaps and criteria for improvement through a continuous cycle of implementation. Thanks to the BI process of strategic advice and baseline assessment of system's vulnerabilities and potential corruption risks, NATO has aimed at achieving a cumulative effect of internalizing policies and procedures. Within a multi-year programmatic framework, NATO is providing tailored support towards consolidation of the outcome of the BI Process. Main efforts are focused on supporting countries implementing peer review recommendations and sustaining change within their defence establishments by means of comprehensive integrity plans and action plans of concrete measures where there are gaps. Programme support included expert visits, workshops/roundtables on specific themes in respective functional areas; education and training; and advice for developing national integrity plans or reviewing existing ones; the identification of solutions and good practice sharing; and the development of national capacity and BI capabilities.

Embedding a Culture of Integrity: the Individual Level

As defined in the NATO BI Policy, integrity relates to socializing norms and values among personnel in institutions.[46] The NATO definition of integrity focuses on the institutional and individual levels of integrity. The two levels constantly interact and reinforce each other through a dynamic process. Institutionalizing integrity reforms requires internal resilience and strength as well as endogenous capacity that cannot be replaced by any

[46] NATO BI Policy, para. 3.

external influence. This understanding underpins NATO's approach to supporting the development of an organizational mindset and a culture of integrity. In 2012, the North Atlantic Council approved the NATO BI Training and Education Plan, establishing the NATO BI Discipline within the Global Programming framework of Allied Command Transformation (ACT).[47] NATO has been working closely with CIDS as the BI Discipline Department Head and the BI Community of Practice to provide a more systematic approach to BI training. Training solutions have been developed and delivered with the support of a growing network of implementing partners, namely CIDS, UK Defence Academy, DCAF, DRESMARA, and the Peace Support Operations Centre of Bosnia and Herzegovina (PSOTC). Online training courses have also been developed for NATO civilian and military staff and these have been translated into several languages for use by partner nations. For instance, the NATO BI Awareness Course has been offered to partners through the e-learning portal of NATO's Defence Education Enhancement Programme (DEEP). In 2024, close to 150,000 Ukrainian representatives from across the whole defence and security sector took the course through the DEEP portal.

The BI Discipline and the use of its tools such as the NATO BI Reference Curriculum[48] support the implementation of integrity and good governance reforms. The education and training activities have provided multiple opportunities for countries to establish a professional corps of functional subject matter experts (SMEs) within their Ministries and Armed Forces, to develop and share knowledge and expertise through peer-to-peer consultations and to train-the-trainers programmes, and to sustain key leaders' engagements needed to maintain a critical mass of reform-oriented champions of change and a professional corps of decision-makers.

Conclusion

The evolution of NATO's strategic approach to integrity and good governance in the defence and related security sector is manifold. First and foremost, corruption and poor governance are recognized as a security threat that needs to be addressed as a critical element of the security paradigm due to its negative impact on defence capabilities, operational effectiveness, and the resilience of democratic institutions and values. Secondly, integrity development has been integrated within the context of NATO's wider policy objectives and the implementation of the Alliance's core tasks. Thirdly, the development of effective, transparent and accountable defence institutions, which are responsive to unpredictable security challenges, including those of a hybrid nature, contributes to the fulfilment of the Alliance's mission to safeguard the freedom and security of its members. This is done in the context of NATO's efforts to provide credible defence and deterrence and in the context of NATO's support to partners to strengthen their defence institutions and capacity.

[47] The Centre for Integrity in the Defence Sector (CIDS) of the Ministry of Defence of Norway is the Department Head of the BI Discipline, while the BI/Governance and Institutions Team at NATO HQ is its Requirement Authority. Both work under the ACT guidance to define training needs and requirements, and to identify existing training solutions or develop new ones.

[48] NATO, *Building Integrity: Understanding the Impact of Good Governance and Corruption on Defence Institution Building — A Reference Curriculum (NATO, 2020).*

6. NATO's Military Concept for Building Integrity in Operations

Thomas Gooch

Introduction

The complexity of modern military operations has expanded significantly in recent decades, demanding not only tactical superiority but also robust institutional integrity. Corruption has emerged as a critical threat multiplier in conflict environments, capable of eroding trust, destabilizing governance, and ultimately undermining the success of military operations. Corruption in the defence and security sector is nothing new, of course. But the fall of Mosul in 2014[1] and the rapid collapse of the Afghanistan Security Forces in 2021[2] are examples of corruption undermining a military force and contributing to its failure in very recent times. Despite vast international investment, the examples demonstrate that military power cannot compensate for the corrosive effects of endemic corruption. These failures highlight the urgent need to integrate integrity, transparency, and accountability in the very concept of operational planning and execution.

The Transparency International Government Defence Integrity (GDI) Index 2020[3] assessed 86 countries against the risk of corruption in five categories – policymaking and political affairs; finances; personnel management; military operations; and procurement. Overall, the GDI 2020 index shows that two-thirds of these countries are at high or critical risk of corruption in their defence and security sectors. Further to this, the military operations category of the index showed the worst performance out of the five categories; this was reflected across all regions and economic groups. Fifty-seven of the 86 countries were assessed as having critical risk of corruption in military operations, with a further 21 having high or very high risk. The consistently poor performance in the military operations category cuts across all regions and income levels, suggesting that the risk of corruption is deeply embedded and systemic, rather than confined to fragile or low-income states. Even in wealthier nations, safeguards and oversight mechanisms often prove inadequate or lack sufficient transparency to prevent abuse. Several key factors contribute to this heightened risk. Military operations are frequently conducted with limited public or parliamentary oversight, frequently justified by national security imperatives,[4] which enables the misuse of resources to go undetected. Decision-making processes related to deployments, targeting, logistics, and the use of force are typically centralized and opaque, offering little accountability. Many armed forces do not provide adequate training on ethical conduct or corruption prevention to personnel engaged in operational environments. This is particularly to be regretted in sensitive contexts like peacekeeping missions or counterinsurgency campaigns.

Operational settings, especially in active conflict zones, further exacerbate corruption risks. The complex and unstable nature of these environments creates opportunities for embezzlement, smuggling, illicit arms trading, and collusion with local power holders. Moreover, operational contracting, such as for transportation, fuel, or local security services, is often rushed due to urgent operational requirements and poor vetting, with a concomitant increase in the likelihood of fraud and exploitation. The implications of corruption in military operations are both strategic and ethical. Corruption can severely undermine the effectiveness of missions and erode public trust, while simultaneously fuelling insecurity and extending the duration of conflict. In fragile contexts, corrupt behaviour among military actors may serve personal or political agendas, intensifying instability

[1] Anna Louise Strachan, "Factors behind the fall of Mosul to ISIL (Daesh) in 2014," *K4D Helpdesk Report* (Brighton, UK: Institute of Development Studies, 2017).
[2] Jennifer Brick Murtazashvili, "The Collapse of Afghanistan," *Journal of Democracy* 33, no. 1 (2022): 40-54, https://www.journalofdemocracy.org/articles/the-collapse-of-afghanistan/; John F. Sopko and David H. Young, Special Inspector General for Afghanistan Reconstruction (SIGAR), "The Factors Leading to the Collapse of the Afghan Government and Its Security Forces," remarks before the 1st Committee of Inquiry (Afghanistan) in the 20th Electoral Term, German Bundestag, March 2023.
[3] Transparency International Defence & Security, "Government Defence Integrity Index (GDI)," 2020 https://ti-defence.org/gdi/ (accessed February 23, 2026).
[4] G. Jasutis, R. Mikova, and K. Cernejute, *Parliamentary oversight of international operations* (Geneva: DCAF – Geneva Centre for Security Sector Governance, 2024) https://www.dcaf.ch/parliamentary-oversight-international-operations.

and human suffering. Additionally, operational corruption can lead to serious consequences such as human rights abuses, loss of credibility in international coalitions, delegitimization of host governments, and the failure of post-conflict reconstruction efforts.

As Amb. Ryan Crocker stated, in an interview with SIGAR (the office of the U.S. Special Inspector General for Afghanistan Reconstruction), ''The ultimate point of failure for our efforts [in Afghanistan] … wasn't an insurgency. It was the weight of endemic corruption.'[5] This simple sentence sums up the point of failure that cost hundreds of billions of dollars and tens of thousands of lives.

The GDI 2020 index, combined with recent experiences in Iraq and Afghanistan, highlights the critical need to address corruption in military operations. In response to the clear threat that corruption poses to military operations, NATO developed the Military Concept for Building Integrity in Operations (BIIO). This concept is born out of NATO's recognition that corruption and poor governance are security challenges that affect NATO's efforts to provide credible deterrence and defence, while projecting stability in the Euro-Atlantic area and beyond. BIIO has turned into a NATO discipline that addresses corruption as an operational risk, focusing on military staff and processes at the operational level. It is guided by NATO frameworks and handbooks, supported by training and subject-matter experts, and requires integrating integrity measures throughout all phases of military operations. The concept, which was approved in February 2021, develops the foundations for BIIO,[6] ensuring that military lines of effort account for and mitigate the risks of corruption in military operations. The concept provides a framework, principles, and guidelines to ensure that BIIO is considered in NATO-led operations, missions, and activities. NATO is now placing increased emphasis on advancing education and training in BIIO. A clear example was the launch of the NATO BIIO Course at the Peace Support Operations Training Centre on 23 June 2025.[7] With expert support from SHAPE, Joint Force Command Naples, FINCENT, and other agencies the programme used interactive learning and real-world case studies to promote integrity and counter corruption in operational contexts.

This chapter provides a brief overview of the concept and its framework. It is structured in four sections: examining the guiding principles of BIIO; the key corruption-related risks to military operations; the operational framework for implementation; and the critical importance of integrating BIIO into training and pre-deployment preparation. It demonstrates that effectively applying BIIO measures not only helps mitigate corruption risks, but also supports sustainable security sector reform, strengthens trust with local populations and partners, and upholds the political and moral legitimacy of NATO operations. In the long term, the integration of BIIO contributes to greater credibility, operational efficiency, and mission success.

1. Principles

In order to provide a clear and simple overarching framework, the concept adopts three principles for BIIO:

Integrity: NATO will act with integrity, both through its individual staff and as an organization. NATO will adhere to international law, practices, and norms and uphold the highest standards. NATO will continue to champion a culture of integrity and will set the standards for partners. This commitment is clearly articulated in NATO's Code of Conduct and the Building Integrity Policy, which jointly establish expectations for personal behaviour, organizational values, and institutional safeguards against corruption.[8] Integrity is not only a normative principle but also a strategic requirement: it builds internal cohesion, reinforces credibility, and strengthens trust within coalitions and within host nations and populations. A case in point was the NATO-led Resolute Support Mission

[5] "Interview of Ambassador Ryan Crocker before representatives of the office of SIGAR," January 11, 2016, https://www.washingtonpost.com/graphics/2019/investigations/afghanistan-papers/documents-database/documents/crocker_ryan_ll_first_interview_01112016.pdf.

[6] North Atlantic Treaty Organization (NATO), *Military Concept for Building Integrity in Operations*, MC 0697, February 12, 2021.

[7] Peace Support Operations Training Centre, "NATO Building Integrity in Operations course successfully concludes at PSOTC," June 27, 2025, https://psotc.org/publication/read/nato-building-integrity-in-operations-course-successfully-concludes-at-psotc2025 (accessed February 23, 2026).

[8] North Atlantic Treaty Organization (NATO), "Building Integrity," last updated 22 January 2025 https://www.nato.int/cps/en/natohq/topics_68368.htm (accessed February 23, 2026).

(RSM) in Afghanistan, where significant effort was made to foster integrity within the Afghan National Defence and Security Forces (ANDSF). Through initiatives coordinated under the NATO BI programme, NATO provided training, mentoring, and institutional support aimed at developing ethical leadership and enhancing accountability in Afghan security institutions. This included anti-corruption education, financial management reform, and internal oversight mechanisms.[9] While long-term structural issues and political instability impeded comprehensive reforms, these efforts contributed to increased awareness and gradual improvement in specific units and ministries, demonstrating the practical impact of promoting integrity in operational contexts.

Transparency: NATO will strive to be transparent in its activities. It will address corruption internally and externally through comprehensive risk management, built upon internal awareness of BI and a comprehensive understanding of specific conditions relating to an operation. Transparency in operations, however, needs to be carefully balanced with the need for Operations Security (OPSEC). An illustrative example is NATO's mission in Bosnia and Herzegovina, which demonstrated transparency through regular engagement with local media, publication of public statements, and coordination with civil society organizations. At the same time, the mission maintained strict OPSEC protocols to protect intelligence and tactical movements.[10] The implementation of these dual commitments–openness with restraint–helped NATO build credibility with the local population while ensuring operational effectiveness.

Accountability: NATO will hold itself and partners accountable for its actions. When working with the private sector, lOs, NGOs and Civil Society, NATO will seek organizations that are transparent and accountable and meet NATO's BI policy in NATO-led operations and missions.[11] For instance, NATO's cooperation with the United Nations (UN) and the European Union (EU) in crisis response and stabilization efforts includes joint initiatives. In Kosovo, NATO's Kosovo Force (KFOR) worked closely with UNMIK (United Nations Mission in Kosovo) and EULEX (European Union Rule of Law Mission in Kosovo). As stated, a key partner for EULEX was the NATO-led KFOR. EULEX and KFOR generally worked closely together at an operational and tactical level, despite the absence of a formal agreement between the EU and NATO.[12]

2. Impact of Corruption on Missions and Operations

In light of the catastrophic failure of the Afghan Government and Security Forces, it may seem that the reasons to address corruption in military operations are obvious. In this regard, the concept highlights four key risks to military operations:

Undermining the desired end state: Corruption will diminish the ability of NATO to achieve sustainable security and governance-related goals. Corruption reduces the ability of the host government to adequately respond to insecurity, and it makes the transition to competent host nation partners challenging. International advisors repeatedly reported difficulties in transitioning responsibility to Afghan counterparts due to patronage networks, ghost soldiers on payrolls, and the misuse of aid. The analysis revealed that corruption substantially undermined the U.S. mission in Afghanistan from the very beginning of Operation Enduring Freedom. They found that corruption cut across all aspects of the reconstruction effort, jeopardizing progress made in security, rule of law, governance, and economic growth. The report concluded that failure to address the problem effectively meant U.S. reconstruction programmes, at best, were bound to be subverted by systemic corruption and, at worst, would fail.[13] This compromised local trust, weakened state legitimacy, and made it difficult for NATO to support a stable handover to competent and credible local institutions.

[9] North Atlantic Treaty Organization (NATO), "Afghan Officials Discuss Building Integrity and Good Governance," news, last updated 18 May 2018; Transparency International Defence & Security, "Government Defence Integrity Index 2020," 2020, https://ti-defence.org/gdi/.
[10] https://www.nato.int/acad/fellow/96-98/combelle.pdf
[11] North Atlantic Treaty Organization (NATO), *Military Concept for Building Integrity in Operations*, MC 0697, February 12, 2021.
[12] European Court of Auditors, *European Union assistance to Kosovo related to the rule of law*, Special Report No. 18 (Luxembourg: Publications Office of the European Union, 2012), https://www.eca.europa.eu/Lists/ECADocuments/SR12_18/SR12_18_EN.PDF.
[13] Special Inspector General for Afghanistan Reconstruction, *Corruption in Conflict: Lessons from the U.S. Experience in Afghanistan*, SIGAR-16-58-LL (Washington, DC: SIGAR, 2016), https://www.oversight.gov/sites/default/files/documents/reports/2020-02/SIGAR-16-58-LL.pdf.

Promoting instability: Corruption hinders the improvement of governance and security architecture in host nations and contributes to instability and wider social grievances. Corrupt politicians and officials create a cycle of low economic growth and poor governmental capacity to deliver effective services. As a result, resentment and disillusionment grow, especially among the poor and the young. In Iraq, for instance, rampant corruption in post-2003 reconstruction efforts led to deteriorating public services, rising unemployment, and a perception that political elites were self-serving. This discontent helped radical groups exploit public grievances and recruit disenfranchised youth.[14] NATO training and capacity-building missions in Iraq had to contend not just with technical shortcomings but with deeper structural issues that corruption exacerbated, undermining security and development gains.

Wasting resources and effort: Corruption through inflated funding within the supply chain increases mission costs. When diverted by malign actors, these funds also have the potential to aid directly an adversary. There were documented cases where fuel contracts were overpriced or supplies were stolen, leading to inflated operational costs. Worse still, stolen resources could fall into the hands of insurgents or adversaries, thereby inadvertently strengthening the very forces NATO seeks to defeat. The textbox below provides additional examples.

Damaging mission credibility: If a NATO-led operation either implicitly accepts or is an unwitting accomplice to corrupt practices, its credibility and reputation within the host nation and on the international stage will be undermined.[15]

Box 6.1. Waste and Corruption in Supporting Local Forces and Economies: Examples from Afghanistan

[Author: Prof. Todor Tagarev]

In 2015, SIGAR published a report stating that the U.S. Department of Defense had spent USD 43 million on a vehicle fuelling station in Afghanistan. The project aimed to show that Afghanistan's natural gas reserves could be used as an alternative to petroleum imports. However, its cost exceeded that of an equivalent project in neighbouring Pakistan by more than 140 times. According to the BBC, the then Special Inspector General for Afghanistan Reconstruction, John Sopko has described this case as ''an outrageous waste of money that raises suspicions that there is something more there than just stupidity. There may be fraud. There may be corruption."[16]

The UK Independent Commission for Aid Impact (ICAI) analysed the GBP 3.5 billion in aid delivered to Afghanistan from 2000 to 2020. Their review stated: 'In complex stabilisation missions, large-scale financial support for the state should only be provided in the context of a viable and inclusive political settlement, when there are reasonable prospects of a sustained transition out of conflict.' Further, it cited governmental documents that 'describe the situation as an extreme form of state capture, which benefited a narrow group of Afghan political elites at the expense of the population at large.'[17]

The United States sanctioned under the Global Magnitsky Human Rights Accountability Act a former member of the Afghan parliament, his son, and 44 related entities, including Western companies, for a corruption scheme allegedly used to divert millions of dollars of U.S. assistance to Afghan security forces. That includes selling bulletproof vehicles to the Kabul elite, providing fuel at artificially inflated prices, fraudulently importing and selling tax-free fuel, and delivering less fuel than required by their contracts.[18]

[14] Mercy Corps, *Investing in Iraq's Peace: How Good Governance Can Diminish Support for Violent Extremism* (Portland, OR: Mercy Corps, 2015), https://www.mercycorps.org/sites/default/files/2019-11/Investing%20in%20Iraqs%20Peace_Final%20Report.pdf.
[15] NATO, *Military Concept for Building Integrity in Operations*, MC 0697.
[16] "Afghan fuel station cost $43m, US military report says," *BBC*, November 2, 2015, https://www.bbc.com/news/world-us-canada-34703279 (accessed February 23, 2026).
[17] "UK aid to Afghanistan Entrenched Corruption and Injustice, Report Finds," *Reuters*, November 24, 2022, https://www.theguardian.com/world/2022/nov/24/uk-aid-to-afghanistan-entrenched-corruption-and-injustice-report-finds (accessed February 23, 2026).
[18] Arshad Mohammed and Daphne Psaledakis, "US puts sanctions on two former Afghan officials for corruption," *Reuters*, December 11, 2023, https://www.reuters.com/world/us-puts-sanctions-two-former-afghan-officials-corruption-2023-12-11/ (accessed February 23, 2026).

All of the above risks can be seen in the Special Inspector General for Afghanistan Reconstruction (SIGAR) report, *What We Need to Learn: Lessons from 20 Years of Afghanistan Reconstruction*, published in August 2021.

Box 6.2. Impact of Corruption on Public Perceptions and the Desired End State[19]

Prior to international forces leaving Afghanistan in 2021, the U.S. Government had spent GBP 83 billion rebuilding the Afghan National Defence and Security Forces. Despite this spending and associated training, a survey of the Afghan people showed that in 2006, 40% of Afghans feared for their personal safety. By 2019, this percentage had risen to 75%.

According to the Special Inspector General for Afghanistan Reconstruction, corruption within the Afghan security sector had long undermined public confidence in the state. The report notes that 'corruption was so pervasive that it significantly undermined the legitimacy and effectiveness of the Afghan government,' and that the diversion of resources and abuse of authority eroded trust in security institutions. Problems such as bribery, 'ghost soldiers,' patronage networks, and the misappropriation of resources weakened operational capacity while simultaneously reducing public confidence in the government's ability to provide security. As the report concludes, widespread corruption not only weakened the Afghan security forces but also contributed to instability by eroding the population's sense of safety and trust in state institutions.

3. BIIO Framework

To provide commanders with a context with which to address these risks, the concept provides the Understand, Plan, Execute, and Assess framework. This framework is not intended to be a constraint for commanders and planners, but rather a handrail that can be applied to any type of planning or operational process. It is intentionally generic so that it can be useful at all levels and all phases of all types of operations.

Understand. As part of the 'understand' phase of the framework, the concept provides five broad areas where it is important to establish a range of indicators to enable systematic data collection and analysis, and their respective groups of indicators. However, these indicators are not exhaustive, and there is often overlap:

- *Environment.* Assesses the broader societal and institutional context shaping corruption risks. This includes perceptions of corruption, public trust in institutions, and societal attitudes toward practices such as nepotism, patronage, or conflicts of interest. It also examines key drivers of corruption, including political dynamics, economic pressures, weak oversight, and informal power structures.
- *Structure of Local Corrupt Networks.* Maps the actors and relationships involved in corruption. This includes identifying key individuals or groups, their roles, hierarchy, and links between political elites, public officials, business actors, and criminal networks.
- *Operating Procedures.* Examines the modus operandi of corrupt networks, including common schemes such as bribery, procurement manipulation, extortion, or misuse of public resources. It also considers how these actors interact with public administration or international missions and how they conceal or facilitate corrupt activities.
- *Vulnerabilities.* Identifies weak points within corrupt networks that could be exploited to disrupt them, such as dependence on key individuals, traceable financial flows, internal rivalries, or exposure to oversight and sanctions.
- *Security Implications.* Evaluates how corrupt practices affect the security environment and mission effectiveness, including impacts on institutional legitimacy, operational capacity, cooperation with local partners, and broader stability.

[19] Special Inspector General for Afghanistan Reconstruction, *What we Need to Learn: Lessons from Twenty Years of Afghanistan Reconstruction*, SIGAR-21-46-LL (Washington, DC: SIGAR, August 2021).

Plan. BIIO efforts must be consistent throughout the planning process. They must be included in the initial political and strategic guidance and direction. If left unaddressed at the strategic level, BIIO efforts and activities planned at the operational and tactical levels may not receive the necessary resources and capabilities. The planning of BIIO efforts must also be done in close coordination with NATO's political BI activities, as well as with other international community stakeholders, such as development organizations, humanitarian actors, and civil society, to avoid competing agendas and duplication of effort.

The concept describes several elements that may well lead to the successful implementation of BI efforts in conflict-affected areas:

- *Establishment of relative security*. Lack of relative security can force commanders to prioritize efforts and resources toward improving security, simultaneously diverting resources away from addressing corruption.
- *Commitment of local leadership to combat corruption*. In conflict-afflicted and fragile countries, government and security institutions may have links to corrupt networks.
- *Public support in the fight against corruption*. The local population can drive social change by making it clear to local leaders that corruption is unacceptable.

Execute. BI efforts require additional considerations that any commanders must account for:

- *Host Nation engagement.* Effective implementation of Building Integrity efforts requires sustained engagement with Host Nation political and military leadership. Securing their commitment to anti-corruption measures is essential for ensuring legitimacy, access to institutions, and long-term sustainability of reforms. Engagement should support awareness of corruption risks, promote ownership of integrity initiatives, and facilitate cooperation between mission actors and Host Nation institutions.
- *Avoidance of competing agendas.* During the execution phase, commanders and mission personnel should coordinate with Host Nation authorities and other stakeholders to avoid duplication of efforts and competing priorities in anti-corruption initiatives. Aligning integrity activities with broader governance and security sector reform efforts helps ensure coherence across different lines of effort and supports mission objectives.
- *Comprehensive coordination with the international community.* The implementation of Building Integrity objectives should involve coordination with international organizations, partner nations, NGOs, and other stakeholders operating in the mission area. Such coordination improves situational awareness, facilitates information-sharing on corruption risks, and contributes to a comprehensive approach to addressing governance and integrity challenges.
- *Institutional knowledge.* Given the rotational nature of deployed forces, maintaining institutional knowledge on corruption risks, networks, and mitigation efforts is essential. Lessons learned mechanisms, knowledge databases, and information-sharing platforms support continuity across rotations and enable more effective monitoring and assessment of integrity initiatives.
- *Influence of external actors.* A comprehensive understanding of the operating environment should include analysis of external actors influencing corruption dynamics, such as regional powers, transnational criminal networks, private economic interests, or other non-state actors. Understanding these influences helps identify drivers of corruption and informs the development of appropriate mitigation strategies.

Assess. Assessment of BIIO efforts is a key component of the BIIO concept. To provide commanders with a clear understanding of success, failure, and progress, a clear process is necessary for capturing and assessing data on BI efforts.

This is a challenging area; a mission or operation needs to have the capacity to:

- *Accurately measure levels of corruption.* Assessment efforts should seek to establish reliable baselines of corruption dynamics within the operating environment. This requires collecting qualitative and quantitative data from multiple sources, including corruption perception surveys, intelligence reporting, institutional audits, and information from international organizations and civil society. Accurate measurement helps identify the prevalence and types of corruption affecting specific institutions or sectors.
- *Measure levels of corruption over time.* Corruption indicators should be monitored through longitudinal analysis in order to track trends and identify whether corruption is increasing, decreasing, or changing in form. Establishing baseline indicators allows mission planners and analysts to compare developments over time and evaluate the effectiveness of integrity-building and anti-corruption initiatives.
- *Establish linkages.* Assessment should examine connections between corruption dynamics and other elements of the operating environment, including governance, security sector performance, organized crime, and political power structures. Understanding these linkages helps identify how corruption interacts with broader instability drivers and how corrupt networks influence institutions, decision-making processes, or illicit activities.
- *Assess issues.* Evaluation should consider the impact of corruption on operational objectives, institutional legitimacy, and mission effectiveness. This includes analysing how corrupt practices affect resource allocation, operational performance, public trust, and cooperation with Host Nation institutions. Such assessments support evidence-based decision-making and inform adjustments to operational planning and anti-corruption strategies.

Access to data on corruption in conflict-affected areas will always be difficult, particularly regarding data related to grand corruption at the political level. This data also needs to be measured in a consistent manner over time, which will enable the establishment of linkages between BI efforts and any changes in corruption levels. Once the data is collected and linkages made, a mission needs to have the capacity and expertise to assess the risks, the validity of planning assumptions, and the establishment of preconditions essential to the success of any BIIO initiatives.

4. Reinforcing Training Efforts

The integration of anti-corruption measures and ethical conduct into pre-mission training is a critical enabler of mission success in today's complex security environments. As military operations increasingly intersect with fragile governance structures and high-risk environments, the ability of personnel to identify, manage, and mitigate corruption risks is essential to safeguarding operational credibility and effectiveness. BIIO brings not only a normative value but is also a strategic necessity, and its incorporation into training and education ensures that NATO forces and partners are equipped with the knowledge, tools, and mindset to uphold transparency, accountability, and good governance in the field. Recognizing this, allied and partner countries have taken significant steps to mainstream BI into their training institutions and curricula. For instance, in Lithuania, before deployment to an area of operations, soldiers attend a course on corruption-related activities and are trained on how to act if they are offered an opportunity to gain illicit benefits and/or to engage in other types of criminal activity. Soldiers who are deployed in international operations, as well as those who have returned from them, complete reports in which one of the questions concerns situations of a corrupt nature. These questionnaires are analysed by the Lithuanian Armed Forces Defence Staff, which provides the Lithuanian Armed Forces Commander with a consolidated assessment and recommendations.[20] Bosnia and Herzegovina and Italy offer compelling examples of how training initiatives can help operationalize BI concepts, transforming policy commitments into practical competencies that support sustainable security outcomes.

[20] Ministry of National Defence of the Republic of Lithuania, *Korupcijos prevencija tarptautinėse operacijose [Corruption prevention in international operations],* March 26, 2024*,* https://kam.lt/korupcijos-prevencija-tarptautinese-organizacijose/ (accessed February 23, 2026).

With support from the NATO Building Integrity Programme, Italy has played a leading role in promoting ethical conduct and anti-corruption principles in NATO operations. In 2019, the NATO Security Force Assistance Centre of Excellence (SFA COE) in Rome hosted the pilot *Building Integrity in Operations* (BIIO) course at Italy's first BI-related initiative. Developed with input from NATO Headquarters and the U.S. Institute for Security Governance, the course aimed to build practical competencies for managing corruption risks in military operations and missions. In 2022, Italy hosted the *NATO Advisory Pilot Course* in Rome, developed under the NATO BI Academic Discipline. This initiative focused on strengthening the role of civilian advisors in supporting defence and security reforms in operational contexts, with a strong emphasis on ethical delivery, transparency, and accountability. The course was shaped with contributions from NATO International Staff, NATO Mission Iraq, ISSAT, and the ICRC, and delivered in partnership with the SFA COE. Through both initiatives, NATO demonstrated its commitment to operationalizing BI, ensuring that BI is not only a policy framework, but a practical tool integrated into advisory work, training, and mission execution.[21] [22]

Bosnia and Herzegovina has institutionalized BIIO principles through annual training hosted by the NATO-accredited Peace Support Operations Training Centre (PSOTC) in Sarajevo. In 2025, PSOTC hosted the second iteration of the NATO BIIO course, developed in cooperation with Joint Force Command Naples (JFCNP) and the Finnish Centre of Expertise for Comprehensive Security (FINCENT), which will be taught annually as a NATO-accredited course starting from 2026 onwards. The BIIO course operationalizes the BIIO concept and enhances BI focal points' ability to contribute to BIIO, including transparency, accountability, counter- and anti-corruption, as well as the evaluation of risks and the impact of corruption across the entire spectrum of operations, missions, and activities within the learners' functional area. One of PSOTC's other key offerings, the BI in Peace Support Operations (BIPSO) Course, is designed to strengthen awareness and operational capacity to counter corruption in military and peacekeeping contexts. The course regularly brings together participants from Bosnia and Herzegovina and other partner countries, with contributions from organizations such as the United Nations Office on Drugs and Crime (UNODC).[23] The course aims to raise awareness of BI and to enhance participants' ability to recognize and counter corruption risks in peace support operations, while promoting good governance in line with NATO and international standards. This recurring initiative demonstrates Bosnia and Herzegovina's continued commitment as a NATO partner to fostering transparency, accountability, and good governance in operational environments.[24]

Conclusion

BI in military operations is by no means the solution to all corruption in military operations. Nevertheless, it provides a common starting point from which commanders and their staff can begin to understand corruption threats and risks, as well as a framework with which to plan, execute, and assess BIIO activities and efforts.

The BIIO concept is operationalized through supporting instruments such as the Allied Command Operations (ACO) BI in Operations Handbook [25] and the ACO BIIO Directive, which translate strategic principles into concrete guidance and procedures for operational contexts. These tools support mission planners in identifying corruption-related risks, mapping integrity gaps, and designing realistic mitigation strategies in line with NATO's broader commitment to good governance, accountability, resilience and mission legitimacy.

Given the demonstrated impact of corruption on mission outcomes–from undermining host nation institutions to wasting resources and fuelling instability–it is essential that BIIO is treated not as an optional add-on, but as

[21] NATO Security Force Assistance Centre of Excellence, *NATO Building Integrity in Operations Pilot Course* (2019), https://www.nsfacoe.org/nato-sfa-coe-and-nato-hqs-co-organized-the-nato-building-integrity-in-operations-biio-pilot-course/ (accessed February 23, 2026).
[22] NATO, *Building Integrity Bulletin* no. 17, – Spring 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/5/pdf/230525-BI_bulletin_17_en.pdf.
[23] United Nations Office on Drugs and Crime (UNODC), "UNODC supports Peace Support Operations Training Centre in Bosnia and Herzegovina with course on integrity," https://www.unodc.org/southeasterneurope/en/all-stories-july2024-unodc-supports-peace-support-operations-training-center-in-bosnia-and-herzegovina-with-course-on-integrity.html (accessed February 23, 2026).
[24] Peace Support Operations Training Centre (PSOTC), *Building Integrity in Peace Support Operations Course*, nd, https://www.psotc.org/Course/Read/14 (accessed February 23, 2026).
[25] *Building Integrity in Operations, Allied Command Operations (ACO) Handbook* (February 2020).

a strategic priority within NATO's operational doctrine. This kind of prioritization would ensure that anti-corruption considerations are embedded from the outset in mission design, rather than being retroactively addressed in response to failure or reputational damage.

Incorporating BIIO effectively will not only reduce corruption risks but also contribute to sustainable security sector reform, bolster trust with local populations and partners, and safeguard the political and moral legitimacy of NATO operations. Ultimately, the successful integration of BIIO measures enhances the credibility, efficiency, and long-term impact of NATO's missions. If applied systematically and supported through leadership commitment and training, BIIO can be a decisive factor in reducing the risk of mission failure and enhancing the prospects for enduring peace and stability in fragile and conflict-affected environments.

Part 3: Corruption Risks and Good Practices in Defence

The third part of this Compendium turns inward, examining how corruption vulnerabilities arise within defence organizations through their own systems. The first article focuses on human resource management, showing how weak HR practices can undermine morale, readiness, and national security. It also presents examples of good practice aimed at reducing these risks. BI as a process is not something that is a duty of a single unit or person. It cannot be delegated; it is the collective responsibility of all public servants. The second article explores military career transition, highlighting how the change from soldier to civilian is a critical period requiring organized support. If it is mishandled, it can become a source of ethical risk, social vulnerability, and exploitation. The whole-of-government care for a successful military-to-civilian transition affects the armed forces' ability to recruit and retain talented people. The veterans' policy is closing the loop of military human resource policy and management in a manner that is not moral and rational. The third contribution analyses public expenditure, including in the military, which is recognized as a major source of vulnerability to corruption. In many countries, most public spending is channelled through public budgets. Therefore, it is important to foresee and prevent corruption risks early in the budget formation process and in implementing the spending side of the budget. The fourth article attempts to examine the integrity issues in defence procurement comprehensively. It sets out internationally recognized principles and examples of good practice for strengthening the integrity of defence acquisition processes, organizations, and personnel. The fifth analysis states that the dual challenge for NATO and partner nations is whether to become more involved in defence business, or to turn more business over to the private sector. Make-or-buy decisions include both traditional short-term defence contracts and longer-term public-private partnerships (PPPs). While there is great potential from partnering, it does entail corruption risks. These chapters explain that BI in defence is not only about systems and strategies. It is about people, their careers, their treatment, oversight of the public expenditure, procurement, PPPs and the choices institutions make at every stage of service.

7. Human Resource Management

Damir Ahmetovic and Roman Rukomeda

Introduction: Human Resource Management in the Public Sector

The essence of Human Resource Management (HRM) is to treat people in a way that encourages them to give their best at work. 'Giving the best' does not only mean maximizing output; it also refers to the adherence to certain standards of behaviour. Public servants should align their behaviour with certain ethical norms both during and after work hours. It is often said that being a public servant is not merely a job; it is a state of mind or a type of mentality that implies the permanent safeguarding of public interest. However, putting public interests first in each and every situation (at work and outside of it) is more easily said than done. Only people who feel valued and supported at work can be expected to do the right thing. Those who are frustrated, demotivated, and disillusioned with the 'reality at work' will struggle to find the motivation to reject opportunities to benefit themselves at the expense of the public. Their surroundings remind them daily that everyone is concerned with their own interests, that higher interests are abused most by those who most loudly defend them, and that there are so many financial gaps that could be exploited if certain principles are not defended rigorously. It is the task of HRM to strengthen institutional resilience by minimizing temptations by implementing procedures, tools, and attitudes that foster a positive work environment, thereby equipping people to resist any propositions that cause harm and lead public servants astray.

In defence institutions, these risks are amplified further. The consequences of corruption and perceived unfairness can be particularly severe. Military and security personnel operate in environments where discipline, trust, and professional integrity are essential for operational effectiveness. When personnel perceive promotion systems, assignments, or resource allocation as unfair or influenced by patronage, morale and institutional loyalty can erode. Disillusioned personnel may disengage from their duties, but in more serious cases they may become vulnerable to illicit approaches that pose direct risks to national security. For instance, a demoralized officer who is repeatedly overlooked for promotion, in favour of less competent but better-connected colleagues, will find it harder to maintain professional loyalty. In a defence environment, where personnel may have access to classified information, sensitive technologies, procurement processes, or operational planning, such disaffection can create opportunities for exploitation. Foreign intelligence services, corrupt contractors, organized criminal groups, or hostile business actors may seek to leverage these vulnerabilities through bribery, coercion, or recruitment attempts.

Modern, public sector HRM should be based on the principles of good governance[1] applicable to all public institutions, including those in the defence sector. Of course, peculiarities linked to the management of military personnel need to be acknowledged. Still, the fact remains that the basic goals of all HRM functions in both public service and the military are more or less the same. Also, the need for democratic civilian control over the military calls for, among other things, convergence of HRM practices between military and public service. This implies the adoption of civilian principles and practices wherever possible and the retention of military-based specifics wherever necessary.

The term 'military-based specifics' refers to the set of approaches for carrying out HRM functions. Several important factors influence these approaches:

- officers and soldiers often discharge their duties in conditions of extreme hardships and are expected to sacrifice their lives if the defence of the country and its citizens are at stake;
- military personnel need to meet physical and mental requirements in a way that is different from regular public servants;

[1] For details on the concept and values of good governance the reader may refer to *Quality of Public Administration: A Toolbox for Practitioners*, (Luxembourg: Publications Office of the European Union, 2015), https://ec.europa.eu/futurium/en/system/files/ged/ke-02-15-267-en-n.pdf.

- attracting people to join the organization that expects so much from them and retaining personnel is a challenging task.

However, the listed factors make no impact on the scope and purpose of individual HRM functions. The goals of both military and public sector HRM include: intelligent HRM planning; adequate job descriptions; effective recruitment and selection; fair and objective performance management; motivating remuneration; competency-building professional development; deterrence-based disciplinary procedures; and continuous integrity-building efforts.

This chapter explores how specific weaknesses in HRM can expose defence institutions to corruption risks and integrity issues. Instead of focusing solely on general inefficiencies and ethical issues, it emphasizes how poor HRM practice may contribute directly to vulnerabilities that hostile actors can exploit. Examples of good practice come from countries where Norway's Centre for Integrity in the Defence Sector (CIDS) implements its projects. There are both NATO members, and those that aspire to achieve that status in the future.

Box 7.1. below provides real-world examples of corruption in military personnel management and the breadth and the increasing severity of the adverse effects it will generate. Chapter 13 in this volume offers another example of assessing corruption risks in human resource management – Operation Kingscliff of the National Anti-Corruption Commission of Australia.

Box 7.1. Examples of HRM-related Corruption and Impact

[Author: Prof. Todor Tagarev]

Draft-dodging via Brokers. In 2023, prosecutors in South Korea had indicted 137 people on charges of attempting to evade mandatory military service. In the so-called 'epilepsy scandal,' draft evaders worked with local brokers to learn how to fake disabilities that would disqualify them from the mandatory draft based on health issues. Such corrupt manipulation of fitness classifications, used by musicians, actors, professional athletes, and sons of affluent people, damages the perceived equity of the draft, with a consequent impact on morale.[2]

Bribery in Recruitment and 'Ghost Soldiers.' The Democratic Republic of Congo has long been plagued by corruption within its armed forces. A common practice is the existence of 'ghost soldiers.' This is a form of personnel management corruption where military commanders or finance officers inflate the number of soldiers in their units, pocketing the salaries and benefits of the non-existent personnel. This practice equates to financial embezzlement and diverts public funds into the pockets of corrupt officers, weakening the force's strength and lowering the capabilities needed to respond to security threats, such as armed rebellions or foreign incursions, and lowering morale.[3] The practice of declaring 'ghost soldiers' on payroll reached extreme levels in Afghanistan prior to the return of the Taliban to power. The Special Inspector General for Afghanistan Reconstruction (SIGAR) has documented fabricated or inflated personnel rolls in the Afghan police and security forces so that officials could appropriate the salaries of 'ghost soldiers' – soldiers and police who had deserted, had been killed, or who had never existed at all. This, among other factors, led to draining of funds,

[2] "South Korea Athletes, Rapper among those Probed over Paying to Fake Illness, Dodge Military Service," *The Straits Times*, March 13, 2023, https://www.straitstimes.com/asia/east-asia/south-korea-athletes-rapper-among-those-probed-over-paying-to-fake-illness-dodge-military-service (accessed February 23, 2026).

[3] Muzong Kodi, *Corruption and Governance in the DRC During the Transition Period* (2003–2006), ISS Monograph Series, no. 148 (Institute for Security Studies, 2008), https://www.files.ethz.ch/isn/103658/mono148fullback.pdf; and Aymar Nyenyezi Bisoka and Koen Vlassenroot, "Corruption in the Congolese Army: Three Lessons for Modern Democracies," *EGMONT Institute*, October 5, 2021, https://www.egmontinstitute.be/corruption-in-the-congolese-army-three-lessons-for-modern-democracies/ (accessed February 23, 2026). For further details on the impact of 'ghost sodiers,' see Ina Kubbe, Nedim Hogic, and Jordan Siegel, "'The Ghost Soldier Trap': How Corruption Undermines Security and Stability," *SSRN*, January 2025, https://doi.org/10.2139/ssrn.5388925.

planning relying on hollow units, and devastated morale. All contributed to the speedy collapse of the Afghan security forces in August 2021.[4]

Bribery for Medical Draft Exemptions. In the summer of 2023, a year and a half into the large-scale war with Russia, Ukraine's President Volodymyr Zelenskyy announced the dismissal of 112 recruitment officers, including all the heads of regional military recruitment centres, in a drive to root out corruption. Officials were accused of taking bribes between USD3,000 and USD5,000 US dollars from men seeking to avoid mobilization. One official in the Odesa region was unable to explain having USD 5 million in savings and a property in Spain. This practice caused mobilization shortfalls and affected troops' morale and public trust in the military. Zelenskyy defined it as cynicism and bribery that, during wartime, was treason.[5] Investigations continued into 2024–2025 and led to the arrest of the army's chief psychiatrist over alleged bribery to issue false exemptions.[6]

Dedovshchina. With the start of the 2022 invasion of Ukraine, middle-class Russians extensively used bribes to avoid the draft for medical reasons or paid money to serve under better general conditions.[7] Further, to attract Russian men into the army fighting in Ukraine, the Kremlin has substantially increased the remuneration package. Russia offers up to RUB 3.4 million (USD 41,900) to convince men to fight in Ukraine, and the amount keeps rising. Top signing bonuses equal nearly five years of typical wages, as Russia's median salary in August 2025 was approximately RUB 58,865 (USD 727)[8]. However, the situation changes dramatically when they reach the frontline. Receiving promised 'frontline' benefits has become more difficult, payments for injuries have been cut, and proving a combat veteran's status is now much harder. Soldiers pay bribes to stay alive. Alternatively, some commanders withhold frontline payment for 'services' on which the life and health of their soldiers depend. Some soldiers have been asked to pay a fee to take leave or to avoid a dangerous mission. There are cases when those who refuse to pay are beaten or threatened with being sent on a mission without a weapon.[9] This fits the traditional *dedovshchina* in the Russian army – bullying, beatings, extortion, hazing, humiliation, and, on occasion, even murder of enlisted juniors. In the ongoing war, the brutality of the Russian military is exhibited by sending repeatedly newly formed units or units staffed with soldiers not trained as infantry in frontal attacks against heavily defended Ukrainian positions. As the casualties mount, corruption and *dedovshchina* have a detrimental impact on morale, unit cohesion, and combat effectiveness.[10]

Loyalty over Merit. Many developing countries struggle to establish a merit-based system for recruiting and promoting military personnel. For example, the UN supported the 2017–2022 National Defence Plan of the Central African Republic, aiming to reorganize its armed forces by enforcing background checks ('vetting') for recruits, and to build a professional army. However, by 2020, the plan unravelled, and the military turned to the 'traditional' practice of ethnic bias, recruiting thousands of soldiers outside formal channels, while

[4] Testimony of John F. Sopko, Special Inspector General for Afghanistan Reconstruction: Hearing Before the Committee on Oversight and Accountability, U.S. House of Representatives, April 19, 2023, https://www.govinfo.gov/app/details/GOVPUB-S-PURL-gpo220906.
[5] Daniel Boffey, "Zelenskyy Sacks Military Recruitment Heads over Frontline Bribes Scandal," *The Guardian*, August 11, 2023, https://www.theguardian.com/world/2023/aug/11/zelenskiy-sacks-all-military-recruitment-heads-over-frontline-bribes-scandal-ukraine (accessed February 23, 2026); "Ukraine Investigates Corruption in Medical Exemptions from Military Duty," *Al Jazeera*, August 31, 2023,https://www.aljazeera.com/news/2023/8/31/ukraine-targets-corruption-in-medical-exemptions-from-military-service (accessed February 23, 2026).
[6] Laura Gozzi, "Ukraine's Chief Army Psychiatrist Arrested on $1m Corruption Charge" *BBC News*, January 21, 2025, https://www.bbc.com/news/articles/cd7dvl0gn1lo (accessed February 23, 2026).
[7] Danish Immigration Service and the Swedish Migration Agency, *Russia – Conscription* (March 2025), https://us.dk/media/fixlsvgr/report-march-2025-conscription-in-russia.pdf.
[8] "How Russia Uses Marketing Tactics to Recruit Soldiers for War in Ukraine" *BBC Monitoring*, November 14, 2025, https://monitoring.bbc.co.uk/product/b0004wrw (accessed February 23, 2026).
[9] Kseniya Kirillova, "Your Money or Your Life: Russia's Frontline Robbery," *Center for European Policy Analysis*, June 9, 2025, https://cepa.org/article/your-money-or-your-life-russias-frontline-robbery/ (accessed February 23, 2026).
[10] Philip Wasielewski, "The Roots of Russian Military Dysfunction," *Foreign Policy Research Institute*, March 31, 2023, https://www.fpri.org/article/2023/03/the-roots-of-russian-military-dysfunction/.

discharging others without explanation, and emphasizing personal and political loyalty in promotion.[11] With decreased national capacity to address counterinsurgencies, Russia's Wagner Group first offered security assistance and then supported or even instigated successful *coups d'état* in the Sahel region.[12] With time, that led to reduced civil liberties, massive human rights abuses, the Kremlin's control over CAR's mineral resources, extracting 'half a billion dollars a year in gold, timber, and blood diamonds', and, ultimately, state capture.[13]

HRM in Action: Main Features and Impact on BI

This section presents the main features of core HRM functions and their potential impact on the Building Integrity (BI) activities. Our understanding of HRM functions, and especially the views on what constitutes good practice, originates from international principles, e.g. SIGMA,[14] and the experience of CIDS in dealing with the subject for the past decade.

Planning Human Resources Needs

The key objective of human resources planning is to ensure that an institution is staffed with the right profile and number of people at the right time. Planning operates on the principle of supply and demand. The demand side refers to the needs of an institution for people with specific profiles. These needs are dependent on the strategic and operational objectives of the institution. Without a sound understanding of the institution's needs, HRM planning is essentially a shot in the dark. The supply side is about the number and profile of people an institution can count on to meet demand. Besides the existing employees, the supply side also includes those who are part of the workforce but are temporarily unavailable (e.g. people on maternity/paternity leave, unpaid leave, away on education or secondments, etc.). These people should be part of the planning process, and the content of the HRM plan should reflect that.

However, it is important not to assume that the term 'supply' refers solely to the number of people. The supply side is first and foremost about having a critical number of people with the competencies required to meet institutional needs. Having ten people and having ten competent people are two very different things. The gap between supply and demand can be credibly analysed only by examining the needs for competencies and, with that information in hand, deciding on the appropriate number of people. The work on getting the people with the right competencies starts by doing a review of the abilities of staff. In many instances, competencies can be acquired by sending staff members for appropriate capacity-building programs. Sometimes, striking a balance between HR supply and demand is a matter of simple reshuffling of staff in order to make sure that their competency profiles and the jobs they do match. Alternatively, institutions may opt to promote from within (especially if there is someone from the lower ranks who represents a viable replacement). However, if an internal solution is not possible, an institution is left with only one option – to go for a public competition and, *de facto*, try to buy the required skills.

Military HRM planning differs fundamentally from civilian workforce planning because it must be closely aligned with national defence strategies, military doctrines, and force-structure planning. Strategic human resource

[11] Enrica Picco, "Central African Republic: Averting Further Fragmentation of the Armed Forces," *International Crisis Group*, May 10, 2022, https://www.crisisgroup.org/africa/central-africa/central-african-republic/central-african-republic-averting-further accessed February 23, 2026).

[12] Samuel Ramani, "Russia Takes its Syrian Model of Counterinsurgency to Africa," *Royal United Services Institute*, September 9, 2020, https://www.rusi.org/explore-our-research/publications/commentary/russia-takes-its-syrian-model-counterinsurgency-africa (accessed February 23, 2026).

[13] Purity Mwambia, "False: With Russia's support, CAR significantly succeeded in combating militants," *VOA Polygraph*, March 4, 2025, https://www.voanews.com/a/false-with-russia-s-support-car-significantly-succeeded-in-combating-militants-/7997777.html (accessed February 23, 2026); Joseph Siegle, "How Russia is Pursuing State Capture in Africa," London School of Economics, March 21, 2022, https://blogs.lse.ac.uk/africaatlse/2022/03/21/how-russia-is-pursuing-state-capture-in-africa-ukraine-wagner-group/ (accessed February 23, 2026).

[14] SIGMA (Support for Improvement in Governance and Management) is a joint initiative of the OECD and the European Union with the key objective to strengthen the foundations for improved public governance. See "About the SIGMA Programme," https://www.sigmaweb.org/ (accessed February 23, 2026).

plans in defence organizations are typically anchored in higher-level strategic guidance, such as national security strategies, defence strategies, and military capability planning documents, which define the missions, capabilities, and force structure required to respond to security threats. These strategic documents translate political objectives into military requirements, including personnel numbers, skill sets, and deployment readiness.[15]

In defence institutions, arbitrary HRM planning can have significant operational and security consequences. Positions may be created (and subsequently staffed) in order to benefit particular individuals or groups whose interests oppose those of the public. Similarly, job posts may be left unfilled due to poor planning or filled through informal arrangements. This could lead to suboptimal organizational performances and open up the institution to corruption.

HRM Planning and Integrity

Decisions made by institutions during the HRM planning process influence consequent decisions regarding recruitment, training, and promotion of personnel. It is in the planning phase that institutions decide on the profile and number of people needed and the way these needs should be met. In that sense, the practice of HRM planning impacts building integrity efforts. If practice is aligned with the approach outlined above, HRM planning can contribute to the development of an integrity-based culture. However, if the practice is poorly regulated and/or outdated, it has the potential to seriously impede BI efforts. This is particularly evident in the development of Non-Commissioned Officers (NCOs), where structured HRM planning supported, for example, by the NATO Defence Education Enhancement Programme, has demonstrated the importance of merit-based career pathways, professional military education, and leadership training in reinforcing integrity at the operational level. A relevant regional example is Montenegro, where reforms in military education and HRM have contributed to the professionalization of the NCO corps. These efforts included the introduction of structured career pathways, transparent promotion systems, and enhanced training curricula emphasizing leadership, integrity, and civilian oversight[16]. The table below demonstrates the main BI-related risks that HRM planning can create, as well as measures for mitigating those risks.

Of note, Non-Commissioned Officers (NCOs) play a critical role in ensuring discipline, operational effectiveness, and the day-to-day implementation of integrity standards within the armed forces. Strengthening NCO corps development through targeted HRM reforms and professional military education (PME) is therefore a key entry point for embedding BI. The NATO Defence Education Enhancement Programme (DEEP) provides a broad range of resources and advisory support aimed at modernizing military education systems, including the development of NCO academies, leadership curricula, and instructor capacity. DEEP-supported reforms typically focus on aligning NCO training with NATO standards, strengthening merit-based career progression, and integrating ethics, accountability, and leadership modules into PME systems. A relevant regional example is Montenegro, where reforms in military education and HRM have contributed to the professionalization of the NCO corps. These efforts included the introduction of structured career pathways, transparent promotion systems, and enhanced training curricula emphasizing leadership, integrity, and civilian oversight. As highlighted in national reform analyses, strengthening the NCO cadre has had a multiplier effect on institutional accountability, as NCOs serve as a critical link between command structures and enlisted personnel.

[15] Michael J. McNerney, Stephanie Pezard, Aimee Aguilar, Samuel Charap, and Lynn E. Davis. *Integrating Allied Military Forces: Lessons Learned and Best Practices.* Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA1115-1.html

[16] Aleksandra Rabrenović, Miroslav Hadžić, and Jovana Misailović, "Specificities of Recruitment and Selection in the Defence Sector – The Case of Montenegro," *Regional Law Review*, no. 3 (2022): 88–102

Table 7.1. HRM Planning and the Risks for Building Integrity

Risks for the institution	Impact on BI	Recommended measures
Planning process based on a weak or non-existent link with the real needs of the institution, including insufficient alignment with national strategic documents	- Misalignment between HRM planning and national security and defence priorities, reducing operational effectiveness and strategic coherence - Risk of poor decision-making in key HRM areas due to the lack of proper analysis - Likelihood of decisions based on arbitrary personal whims - Inconsistency of actions (i.e. improvisation as a substitute for regulation) - Creation of unnecessary costs (e.g. remuneration package for the future job holder, administrative cost of recruitment and selection)	- HRM Planning procedure must be well-regulated - The process of planning should recognize both qualitative and quantitative sides of the need for personnel - Recruitments should be linked to HR plans, and employment outside the HR plan must be kept to an absolute minimum - A checks-and-balances mechanism should be introduced in the process of approving HRM plans - The process of planning should be coordinated by the HRM unit, with the key inputs coming from the unit managers
Automatic replacement of outgoing staff	- Risk of poor efficiency in the work of the institution as a result of neglected analysis of the demand for people and the most optimal way to supply them - Sub-optimal allocation of human and financial resources (by going for the automatic replacements, which *de facto* disregard priorities)	- Focus should be placed on acquiring/retaining competencies; people leaving does not necessarily imply the loss of competencies - Promote from within whenever possible; recruit from outside whenever necessary (merit-based approach must be ensured in any case) - Identify individuals with the right motivation and potential to go for development courses/ programmes

Designing and Describing Jobs

Individual job posts are described as defining duties, responsibilities, reporting lines, and the requirements a job holder must meet to successfully carry out their duties and responsibilities. When a job post is being created for the first time, the process of defining its content (i.e. tasks and responsibilities) is called job design. Later on, when the content is in need of updating, it is done by performing some form of job analysis, i.e. the activity of collecting and analysing job-related data. Decisions to establish (or abolish) work posts should be based almost exclusively on the functional needs of an institution. These needs should be identified based on current circumstances as well as projected future ones. Furthermore, for the functional needs to warrant the creation of a new work post, they need to be permanent (or at least long-term); otherwise, putting in place a new work post could prove to be economically unfeasible. Once the decision to create a new work post is made, it is important

to design it in such a way as to make it meaningful and challenging for the future incumbent. Jobs whose duties are repetitive in nature and which bring little challenge and variety will impact negatively on the incumbent's motivation and are almost certain to cause engagement issues.

When it comes to amending job descriptions, institutions usually rely on job analysis interviews with the existing job holders (or their immediate supervisors). In the course of the job analysis exercise, trained job analysts receive information that often goes beyond the duties of a particular job and provide an insight into wider organizational issues and challenges. Institutions that face issues with the accuracy of job descriptions risk causing problems related to work duplication or work silos.

In parallel to this, poorly written and/or outdated job descriptions create communication problems that often result in strained interpersonal relations among staff members. In the defence sector, poorly written or deliberately manipulated job descriptions can have serious implications. For instance, a job post that grants access to data on sensitive procurements, if inadequately defined, may allow a job holder to exploit opportunities for personal or external gain. Furthermore, writing or re-writing job descriptions to fit concrete individuals can result in critical jobs being filled by underqualified staff, which could weaken national defence readiness.

Job Descriptions and Integrity

Table 7.2. Job Descriptions and the Risks for Building Integrity

Risks for the institution	Impact on BI	Recommended measures
Developing job descriptions to suit a person not the job	- Manipulating the content of job descriptions undermines the principles of equal opportunity and meritocratic selection - Risk of poor efficiency in the work of the institution (as a result of neglecting the functional duties and responsibilities as the basis for developing a job description)	- Develop the job description based on functional duties, not the person; standardize the format of job descriptions and issue instructions related to the nature of its content (i.e. length and style) - Obtain the job data from the actual job holders and use job analysis techniques - Assign the HRM unit the responsibility to coordinate the development of job descriptions and to control content
Poorly defined content of job descriptions	- Risk of poor individual performance (as a result of disengagement caused by issues like unclear duties, responsibilities, and reporting lines, as well as a mismatch between what the job description states and what the person actually does); poor individual motivation can lead to work negligence and tolerance for ethically questionable issues.	- Obtain the job data from the actual job holders using job analysis techniques - In case of a new job, immediate supervisors should be in charge of providing the content (in line with functional needs) while the HRM unit should be in charge of transforming that content into a proper job description

A job description is a central HRM document. It is the basis for all core HRM functions – planning, recruitment, performance assessment, remuneration, and professional development. Therefore, job descriptions should be credible: they should reflect actual duties and support institutional goals, and they should be updated regularly. This reduces the risk that descriptions are tailored to specific individuals rather than to the role's functional duties and responsibilities. Also, credible and updated job descriptions are likely to prevent work stress, frustration, and disengagement among employees. On the other hand, poor job descriptions are bound to create various operational issues (i.e. this is not my work, it is not stated in my job description, etc.). These, too, are likely to cause an unhealthy work environment, which in turn undermines BI efforts.

Recruitment and Selection

The ability of public service institutions to respond to the demands of daily work depends first and foremost on the ability of individual staff members to carry out their job duties and responsibilities. One of the key requirements for all public sector institutions is to employ people based on principles including equal opportunity, non-discrimination, merit, and transparency. To secure adherence to these principles, public institutions are required to implement competitive procedures. A typical procedure consists of two stages: recruitment and selection. Recruitment refers to activities aimed at building a pool of qualified candidates, while selection focuses on assessing those candidates in a fair and transparent manner. The paramount objective is to adhere to the principle of merit, which means that the best (i.e. highest scoring) candidate is appointed for the job.

However, safeguarding the principle of merit is an uphill task considering that, in many countries, public sector jobs are regarded as highly desirable and, as such, serve as a 'bait'. Political parties and other interest groups and individuals use such positions in their attempt to generate support for their interests. Needless to say, in a large number of cases, their interests run directly against those of the citizenry.

Selection is highly dependent on the quality of applicants that institutions manage to attract through recruitment activities. Hence, the need for job vacancies to be placed in the media with the highest circulation; in today's context, it means various internet portals and social networks. As traditional media converge towards the internet, the trend is to place vacancy notices online, given the far greater reach of internet portals and social networks (e.g., LinkedIn, Facebook, etc.) compared to traditional media. At the same time, the cost of digital advertising is significantly lower.

Apart from the need to build a pool of qualified candidates, the selection process needs to be based on sound testing methods. The focus must be on assessing applicants' demonstrated ability to meet the job demands (i.e. competency-based selection) instead of relying solely on formal qualifications (i.e. degree, various certificates, etc.). This is especially important in developing countries, where systems of accreditation at the tertiary education level are underdeveloped, offering little assurance about the quality and credibility of formal qualifications.[17]

In a nutshell, competency-based testing involves assessing applicants through a series of tests, typically comprising written and oral examinations. The aim is to test candidates' technical and behavioural competencies by asking questions related to duties and responsibilities (i.e. usually essay-type questions about concrete job-related situations or problems), as well as questions related to behavioural competencies (e.g., result-orientation, ability to work under pressure). This is usually done in the format of an interview. Selection committees score the candidates using pre-defined criteria. The highest-ranking candidate should be offered a job.

[17] For more information on this topic see Emanuela Di Gropello, "The Future of Higher Education: Four Critical Questions for Policymakers in Developing Countries," *World Bank Independent Evaluation Group*, October 2, 2018, https://ieg.worldbankgroup.org/blog/future-higher-education-four-critical-questions-policymakers-developing-countries; and Pavel Zgaga, Manja Klemenčič, Janja Komljenovič, Klemen Miklavič, Igor Repac, and Vedran Jakačić, *Higher education in the Western Balkans: Reforms, developments, trends. Key findings from field research* (Ljubljana: Faculty of Education, University of Ljubljana, 2013), https://repozitorij.uni-lj.si/IzpisGradiva.php?id=17531.

From the perspective of defence institutions, non-meritocratic recruitment carries an added layer of risk. Unlike in much of the public sector, military personnel systems typically rely on recruitment at entry level followed by structured, rank-by-rank promotion, often influenced by seniority, age, and formal requirements. This makes early-stage recruitment decisions particularly critical, as deficiencies at entry level may persist and compound throughout a career. If selection procedures are manipulated to favour candidates with personal or political ties, individuals may enter the system without the required competencies. In strategic posts such as data management, intelligence support, or defence procurement, this creates risks not only of inefficiency but also of serious breaches of national security. For example, appointing the wrong candidate to a procurement position may lead to the leakage of sensitive contractual data.

Recruitment and Selection and Integrity

This is undoubtedly the most sensitive HRM area when it comes to corruption risks. Ruling factions have always been interested in controlling the processes of hiring and firing, as it enables them to count on the kind of subordinate staff whose main qualities are loyalty and obedience. In the context of developing countries, the efforts should focus on making the process transparent and as manipulation-proof as possible. Listed below are the main risks in this area, which, if left unaddressed, could cause significant damage to building integrity initiatives.

An example from Albania demonstrates an approach to the selection process that makes it hard for the decision-makers to manipulate the results of the process.

Box 7.2. Example of Good HRM Practice: Selection of Public Servants in Albania[18]

Albania is the first country in the Western Balkans to introduce the process of pool recruitment. In a nutshell, the process centres on recruiting and selecting a larger number of people (i.e. the logic is to go by families of jobs, for example, legal professionals, HRM, procurement specialists, etc.). These individuals go through examinations and are ranked by the score they achieve. As and when a suitable vacant position appears (anywhere within the public administration), the highest-ranking candidate is given the first choice to get the job, and then the second one, and so on until all the successful candidates are employed.

Apart from rewarding the first-ranked candidate, this approach neutralizes the influence of individual institutions in the process, which reduces the risk of politicization and favouritism.

In addition, Albania has simplified the application process for public service jobs, allowing everything to be done online. Most documents are required only from the selected candidates, and the Department for Public Administration has been very proactive in assisting candidates to apply. In this way, the avenues for manipulation in the course of the application process are minimized, and the simplicity and affordability of the whole process are ensured.

[18] Jan-Hinrik Meyer-Sahling, Kim Sass Mikkelsen, Christian Schuster et al., *Making Merit Recruitment Work: Lessons from and for the Western Balkans* (Danilovgrad, Montenegro: Regional School of Public Administration, 2020), https://www.respaweb.eu/download/doc/Making+Merit+Recruitment+Work_Lessons+from+and+for+the+WBs.pdf/77467aa94a0ed147ce90b1747143f850.pdf.

Table 7.3. Recruitment and Selection and the Risks for Building Integrity.

Risks for the institution	Impact on BI	Recommended measures
Reducing the quality of competition by deliberately posting vacancy announcements in media that do not have the highest circulation	- The principle of equal opportunity and equal access to public jobs would be seriously harmed - A limited pool of candidates will affect the selection decision, which will in turn affect the quality of the future incumbent's work - Waste of public money	- Introduce provisions that compel institutions to place vacancy announcements in the media with the highest circulation and the best 'value for money' ratio (including internet media and social networks)
Poor choice of testing methods	- Merit principle seriously compromised - Waste of public resources at the stage of testing	- Introduce competency-based tests consisting of written and oral exams - The written exam should be in an essay form, focusing on the required technical competencies - Use an oral exam (i.e. interview) to test behavioural competencies
Appointment decision left solely to the head of the institution	- The risk of arbitrariness in deciding on the appointment (as a result of politicization or advancement of personal interests) - Risk of neglecting principles of non-discrimination and merit - Risk of wasting public resources (if the candidate other than the first ranked one is appointed);	- Introduce a regulation that the appointment of the first-ranked candidate is mandatory - In specific situations (for instance, to reduce gender imbalance), an institution may opt not to select the first-ranked candidate [19]
Lack of transparency	- The risk of favouritism and protectionism in the work of selection panels - The risk of neglecting principles of non-discrimination and merit - The risk of generating a negative image of the public service among citizens	- Introduce increased transparency in the testing process - Possible measures may include audio-video recording of the whole testing proceedings or allowing representatives of civil society organizations to monitor the process
Fraudulent enlistment	- Admission of unqualified or unsuitable personnel into the system - Increased risk of misconduct, disciplinary violations, or insider threats - Undermining of merit-based recruitment and institutional credibility	- Strengthen background verification and vetting procedures - Introduce stricter accountability mechanisms for recruiters and supervisors

[19] This should be considered only in exceptional cases when imbalances within the institution are really significant (e.g. gender imbalance) but even in such cases it should be done in a controlled way.

Fraud in military referral bonuses	- Distortion of recruitment incentives and priorities - Financial losses and misuse of public funds - Risk of favouritism, collusion, and corruption within recruitment structures	- Introduce transparent tracking and verification mechanisms for referral claims - Separate recruitment and incentive approval functions - Conduct periodic financial and procedural audits of referral programmes

Management of Individual Performance

Performance management is essentially a double-track process: on the one hand, the institution is trying to get the best results from people and, on the other, it provides them with the learning and development support to ensure their continuous professional growth. Therefore, performance management benefits both the institution and the individual. Managing employees' performance is critical for their motivation. Individuals need feedback from their superiors not only to know how well they are doing at work but also to learn where they can make improvements. This is the basis for people's motivation and engagement at work. However, solid individual performance does not automatically translate into good institutional performance. Other factors, such as inadequate regulation or a lack of political support, can stand in the way. Yet, behind every solid institutional achievement stands a good performance at the individual level.

In reality, performance management is often reduced to just one single element: performance appraisal. Other elements, such as setting objectives, monitoring performance, and providing support, often get marginalized or become insignificant in the appraisal procedure. This is one of the main reasons why, in many instances, people complain that the entire practice is, in essence, a formalistic exercise that fails to deliver its two chief outcomes: motivated and well-trained staff.

The weak link between performance results and rewards or bonuses is often cited as the reason for the negative view of the practice among public employees. While in principle the link between performance and rewards is justifiable, managers have a great deal of responsibility to ensure procedural fairness. Otherwise, the appraisal results would lack the necessary credibility. For instance, giving rewards to individuals who merely carry out their tasks and responsibilities (even if they do it in a timely and efficient manner) begs the question of what the purpose of regular salaries is. Average performance? If salaries are not sufficient to compensate for good performance, what, then, are we paying for? In the military environment, rewards and compensation are not always expressed in purely monetary terms. They may also take the form of promotions, prestigious assignments, honours such as medals and unit citations, and other forms of recognition. All of these elements should be understood as integral components of the incentive structure of the modern military professional, shaping motivation, performance, and integrity alongside financial remuneration. Rewards must be based on standard, transparent criteria and should stimulate excellence. Otherwise, institutions risk undermining the basic value system and blurring the lines between ordinary and exceptional individual performance. There is hardly anything extraordinary about an employee who carries out competently the prescribed duties and responsibilities. It is important to mention here the issue of inflated marks that stem directly from managers' inability, or lack of willingness, to distinguish between poor, average, and high performers.[20]

Performance appraisals that reward loyalty over merit can place unqualified staff in positions of responsibility. In command roles or sensitive operational assignments within defence institutions, this might jeopardize

[20] Regional School of Public Administration, *Individual Performance Appraisal of Employees in Central Public Administration in Western Balkans: Baseline Analysis* (November 2018), https://www.respaweb.eu/download/doc/Performance+Appraisal+Study%2C+Nov.+2018.pdf/8cb59b0dc64e80a29a95d0c6100e765f.pdf. More on the fairness of rewards can be found in Publications Office of the European Union, *Pay-for-performance in the civil service of the EU* (Luxembourg: Publications Office of the European Union, October 14, 2021), https://ec.europa.eu/info/sites/default/files/ht0921294enn.en_.pdf.

missions or compromise classified information. An officer promoted based on personal relations rather than performance may not only fail to deliver. The choice might also alienate capable subordinates, thereby increasing the risk of disengagement or ethical issues within the unit.

Performance Management and Integrity

Table 7.4. Performance Management and the Risks for Building Integrity.

Risks for the institution	Impact on BI	Recommended measures
Abusing performance assessment by giving the highest marks to those who are loyal, instead of those who give the best performance	- Practicing a form of veiled bribery - Establishing a culture of loyalty to individuals, not to the institution or the public	- HRM unit to enable anonymous reports about harmful HR practices - HRM unit to carry out periodic staff satisfaction surveys, checking, among other things, opinion about the objectivity of the performance appraisal
Cancelling performance differences among employees by giving highest marks to everyone	- Undermining the performance culture - Ruining ethical norms (i.e. lack of fairness)	- Government should issue guidance recommending marks quotas - Government should assign responsibility to the relevant institution to review the distribution of marks - Institutions that end up breaching the quotas to put 'on-hold' decisions to give out bonuses or rewards until they produce justification (for the breach of quotas), which will satisfy the Government.
Weak or non-existent link between performance assessment and other HRM functions	- Undermining performance culture - Risk of arbitrary decision-making (i.e. non-merit promotions and training, unjustified spending)	- Introduce the provisions in secondary legislation that create a firm link between performance appraisal results and decisions regarding the promotion, allocation of bonuses/rewards, and sending people for training

Individual performance results constitute the basis for important decisions: promotion; allocation of bonuses; and selection for professional training. These decisions risk being used by managers in an unethical way to secure the loyalty and obedience of subordinate staff. The logic is clear: those who are loyal and obedient will get the highest marks (regardless of actual performance), and this will boost their chances for promotion and put them in line to receive bonuses/rewards and be selected for training courses (especially courses abroad). Furthermore, managers may decide to allocate the highest marks to all employees in an attempt to appease

them. In this way, all staff will have the same marks and will have the same chance for promotion, bonuses, or training. However, this approach would be fragile and would gradually erode the culture of performance, as individuals who work more or better will surely seize the first opportunity to leave this kind of an environment.

Career Management

The ability of public institutions to attract and retain people depends to a great extent on their ability to offer solid career prospects. These prospects may come in the form of career growth opportunities (i.e. advancing from the current post to a higher one) or some other options that imply improvements in the professional side (e.g. education, professional training).

However, career development in public institutions must be aligned with the principles of merit and equal opportunity. In other words, moving up the ladder (career growth) is subject to promotion, which, in turn, rests on the existence of open competitions designed to ensure that the best candidate gets the job. Military and police officers may be exceptions here as they are promoted based on decisions of assessment boards taking into consideration criteria such as years of service, quality of work performance, current rank, and leadership competencies.

Apart from respecting the interests of the public, the process of individual career development must also be in line with the needs of the institution. An institution can support a person's career goals only if those goals add value to the work of the institution. Otherwise, public money may be spent on career objectives of no relevance to the institution. Such financial commitments can hardly be justified. However, an individual can always decide to dedicate their own time and money to obtain certain professional credentials that hold relevance for their long-term career goals.

Finally, career goals should be challenging but realistic. They should be set in consultations with the immediate supervisor, preferably in the course of a performance appraisal interview. Career growth in the public sector is subject to prescribed requirements, and any hopes for quick advancement are unrealistic. Also, career objectives should be organized in line with certain institutional priorities. For instance, if an individual's aspirations for development clash with those of the institution, the advantage should be given to the institution since its priorities hold higher relevance for the needs of the public.

In defence institutions, career stagnation due to favouritism or arbitrary decision-making may result in officers becoming cynical, disengaged, or prone to manipulation. An officer blocked from advancement, despite strong qualifications and loyalty, might feel justified in bypassing official channels or leaking information as a form of protest or retaliation. This creates a fertile ground for both internal dysfunction and external exploitation.

Career Management and Integrity

Career growth in the public sector is expected to take place mainly through promotion. That process warrants some competitive procedure and strict adherence to the principles of impartiality and merit. However, in some instances, the legislation related to promotion gives extensive authority to the head of the institution. This may result in risks of arbitrary promotion decisions. In addition, provisions that enable transfers of staff may be utilized for discipline, e.g. 'if you don't do this, I will transfer you to that place.' Finally, there is always a possibility for the superior to slow down or even block the career progression of individuals who do not show sufficient 'cooperation.'

Table 7.5. Career Management and the Risks for Building Integrity.

Risks for the institution	Impact on BI	Recommended measures
Arbitrary promotion decisions	- Undermining the principle of merit - Discrediting the culture of performance	- Regulate promotion matters in a way that will make the final decision the result of a group decision (i.e. via a promotion panel) rather than the discretion of a single person
The use of transfers for the purpose of rewarding/ punishing people	- Veiled bribery - Establishing a culture of loyalty to individuals, not to the public	- The HRM unit should enable anonymous reports about harmful HR practices, including in the use of transfers - The HRM unit to carry out periodic staff satisfaction surveys, checking, among others, the opinion about the fairness of transfer decisions
Deliberate attempts to unjustly speed up/slow down (or even block) the career advancement of staff members	- Undermining trust in fair and just career opportunities, leading to the loss of trust in the system as such - Discrediting the principle of merit and the culture of performance	- Reduce the decision-making authority of a single person - Empower decision-making by committee and based on clearly set criteria for career advancement

Professional Development

Professional development refers to the overall growth of an individual in terms of ability, understanding, and awareness. It is essentially the culmination of all our learning efforts, regardless of the approach we take. Often, lessons learned informally in private life become a valuable part of our professional development, too. This is a lasting process, but for some, it stops with retirement, while others continue to improve themselves professionally as a matter of personal interest or as a hobby.

Professional development is often used as a synonym for training. This is incorrect because training is a more specific concept that involves the systematic acquisition of competencies (knowledge, skills, and attitudes) necessary for a person to perform a given task or job effectively. As such, training is just an integral part of professional development; it is simply one of the ways to learn and, in that way, to contribute to professional development.

Undertaking some form of professional development makes sense only if it stems from the needs of the institution. Hence, it is absolutely critical for institutions to carry out a proper needs analysis. Training and other forms of learning that have no basis in the real needs of the institution are a waste of taxpayers' money. Besides, in addition to knowing the needs for professional development, an institution should also come up with realistic learning objectives and a well-thought-out design and form of learning. In the end, training (or some other form

of professional development) needs to be carried out in a manner appropriate for public service, i.e. adhering to the principles of equal opportunity, transparency, and merit.

Finally, since professional development undertakings imply spending taxpayers' money, related decisions should be scrutinized through some form of evaluation. Apart from the regular post-training reports written by participating employees, it is strongly recommended that institutions regularly conduct training impact evaluations to assess the effects of the learning experience on the individuals and the organization. In the context of defence institutions, professional development decisions are of critical importance. Sending unqualified or politically favoured individuals on attractive training courses may weaken the competencies available for the institution. It may also impact its credibility internally and with international partners. Moreover, exposure to sensitive international environments without proper vetting increases the risk of espionage or information leakage.

Professional Development and Integrity

Decisions related to training and other forms of professional development can also be subject to corrupt practices. Again, the main risk is that decision-makers will prioritize sending loyal and obedient individuals for training over those who could benefit the most. In addition, other training decisions, such as the selection of topic and/or participants, risk being made without much regard to the interests of the institution.

One way to reduce the probability of corruption is to offer centralized (online and in-person) training courses, such as those provided by the Building Integrity Training and Educational Centre (BITEC), Ukraine (see Box 7.3 below).

Box 7.3. Good HRM Practice: BITEC's e-Learning Training System in Ukraine

eLearning training has grown in popularity in recent years, and training centres across the globe have expanded their reliance on this method. The Building Integrity Training and Educational Centre (BITEC) at the National Defence University of Ukraine is one such institution. Recently, BITEC has adapted its programmes to meet the needs of its students, utilizing modern technologies to effectively reach the target audience. They have managed to diversify the way they deliver their training programmes by creating a host of online courses, interactive educational and practical games, as well as applications dealing with anti-corruption for smartphones and hand-held devices.

BITEC's swift re-orientation towards e-learning has been a success:

- In the second half of 2021, about 20,000 students registered for some of the offered courses, and more than 12,000 completed the course successfully.
- The courses gained instant popularity among students, as they could choose their own most appropriate timing for the mid-term and final exams.

A separate element of this level of training is the online course called Stop Corruption. In a clear and attractive form, it provides information on theoretical and practical issues with BI and the fight against corruption, taking into account recent changes in national legislation.

BITEC implements its activities through the assistance of the UK Ministry of Defence and in cooperation with the UK Defence Academy and CIDS.

Further information on BITEC's work is available at https://bitec.com.ua/en/main-english/.

Table 7.6. Professional Development and the Risks for Building Integrity

Risks for the institution	Impact on BI	Recommended measures
Using training as a way to reward loyal staff	- Veiled bribery - Establishing a culture of loyalty to individuals, not the public	- HRM unit to enable anonymous reporting on harmful HR practices, including how employees are selected for training - HRM unit to carry out periodic staff satisfaction surveys, checking, among others, opinions about the fairness of training decisions
Making training decisions irrespective of institutional needs	- Misappropriation of public resources - Disregard for the interests of the institution	- Introduce obligatory standard training needs analysis (TNA), which recognizes needs at institutional, departmental, and individual levels - The HRM unit should monitor/approve training proposals based on annual TNA

Disciplinary Management

Disciplinary management refers to the activities designed to make public servants work and behave in line with rules and regulations. It is crucial to recognize that discipline does not always require a corrective approach, as preventive measures can effectively address issues before they escalate into full-blown problems. For instance, managerial mediation can be used as an informal process to resolve the problems between employees.

However, once disciplinary proceedings are launched, public service institutions are obliged to ensure that there is a proper disciplinary hearing and that the person under disciplinary investigation is allowed to explain their side of the story. Also, it must be possible to challenge the decision of the employer before higher instance authorities.

Ethics, Discipline, and Integrity

The main integrity risk in this area is that public officials may act contrary to rules and regulations willingly. To commit an offence due to a scarcity of information or a lack of capacity to handle a task is different from the situation where an individual knowingly and willingly takes actions that harm the institution. Both are disciplinary issues and should be addressed as such, but the latter is an ethical issue, too. Manifestations of unethical decision-making are more or less known: conflict of interest, bribery, politicization, nepotism, and arbitrariness are just some of those that citizens complain about. However, BI efforts in the past have been directed primarily to identifying the forms (and to a lesser extent, sources) of unethical behaviour and how to remedy these tendencies.

There are very few studies that examine the root causes. People are not inherently bad, so why do they make decisions that they know are harmful to the public interest, and what makes them resistant to the feeling of guilt

afterwards? CIDS is undertaking considerable efforts to uncover these root causes for the benefit of future BI efforts.

Undisciplined or unethical behaviour that goes unchecked can have significant operational consequences for defence institutions. If senior officers tolerate problems due to personal loyalty, or if disciplinary mechanisms are misused to suppress whistleblowers, the result can be a culture of silence that allows corruption or security breaches to flourish. A sustained deterioration of professional standards can lead to even more serious consequences beyond corruption, including abuse of rights and criminal conduct.

Box 7.4. Good HRM Practice: Assessing the Risk of Corruption at Individual Work Posts.

The methodology is based on a simple logic that the relative risk of corruption depends on two factors: a) the probability that the corrupt activity may occur; and b) the strength of the impact it can cause (if it occurs). Jobs are assessed using the job descriptions, and, therefore, it is of critical importance that these documents be accurate and up to date.

Criteria used for assessment include: 1) level of authority; 2) access to information and resources; 3) level of discretionary decision-making/unclear or missing legal provisions; 4) effective monitoring and control mechanisms; 5) degree of exposure to undue pressure; 6) rigorous sanctions. The table below shows how corruption probability and potential impact are scored before being multiplied (e.g. CP = 4, PI = 5; Sensitivity level (SL) = 4 x 5, SL = 20). The scoring is done for each criterion, which means that a particular job may score very high SL when it comes to, for instance, access to information, but moderately high on the criterion 'Existence of rigorous sanctions.'

Corruption probability (CP)	**Score**	**Potential impact (PI)**	**Score**
Minimal probability of corruption activity	1	Insignificant impact	1
Low probability of corruption activity	2	Low impact	2
Moderate probability of corruption activity	3	Moderate impact	3
Considerable probability of corruption activity	4	Major impact	4
Very high probability of corruption activity	5	Devastating impact	5

The results are classified into one of the five sensitivity categories: 1) minimal; 2) low; 3) moderate; 4) high; 5) extreme. Jobs that fall into categories 4 and 5 warrant measures such as unannounced inspections, spot checks (in relation to asset declarations), and job rotations. The methodology has been applied in Bosnia and Herzegovina (Ministry of Defence, 2014), Kosovo (Ministry of Defence, 2021 and Ministry of Interior, 2022), and is included in the *Anticorruption Program 2025-2026* of the Ministry of Defence of Ukraine through which it will be tailored to the local context.

For more information about the methodology, contact CIDS at: cids@fd.dep.no.

Table 7.7. Disciplinary Management and the Risks for Building Integrity.

Risks for the institution	Impact on BI	Recommended measures
Issuing illegal orders/ instructions	- Disregard for the interests of the institution (i.e. corruption) - Depending on the nature of the order, it can seriously harm public interest	- Introduce legal provisions that will make it mandatory for public servants to refuse orders/instructions that are in breach of any regulation - Introduce strict fines for those who issue and/or carry out illegal instructions
Entering into arrangements that constitute a conflict of interest	- Advancing private instead of public interests - Disillusionment with ethical norms among employees	- Introduce legal provisions that will make it mandatory for public servants to refuse orders/instructions that are in breach of any regulation - Introduce strict fines for those who issue and/or carry out illegal instructions
Manipulation of the disciplinary proceedings	- Erosion of trust among employees in the justice and fairness within the system - Public service is acquiring a negative image among citizens	- Make the work of disciplinary committees more transparent (e.g. allow civil society organizations to request that their representatives monitor proceedings)

Conclusion

HRM can play a significant role in forging integrity in the public sector. Since this is a function that deals with people and their needs, issues, and perceptions, HRM staff should be able to identify the institution's sensitive spots as well as its strengths and weaknesses *vis-à-vis* BI. Moreover, HRM professionals should focus their attention on providing public servants with the support, advice, and, when necessary, protection. Of course, for HRM to have the credibility to play this role, its own integrity record has to be impeccable, and HRM officials have to be seen as role models in integrity.

However, the success of HRM as a champion of integrity depends on one more thing: it has to grow into a strong managerial function and it has to be seen as such by both the leadership and employees. As long as HRM is confined to mainly administrative work, it will be perceived as being marginal (even weak) and, consequently, unable to assert itself as a bearer and promoter of integrity. HRM needs to evolve into a true strategic function that adds specific value in institution building. Therefore, HRM's relevance as an organizational function and its credibility as a champion of integrity both depend on the ability to carry out the act of transformation.

In the defence and security sectors, this transformation is not only desirable but urgent. Weak or misused HRM systems can lead to significant vulnerabilities in state institutions, including in areas related to insider threats in procurement or the management of sensitive data. The integrity of defence systems starts with the integrity of people and how those people are selected, trained, promoted, and held accountable.

Meanwhile, it is important to stress that HRM may be in the driving seat when it comes to organizing BI efforts in an institution. Still, BI as a process is not something that is a duty of a single unit or person. It cannot be delegated; it is the collective responsibility of all public servants. However, decision-makers must ensure that this responsibility does not become too burdensome for regular public servants to bear. We must not expect public servants to act as heroes in order to stop corruption. Those in power and those who draft and enforce laws have a duty to make it easy and natural for public servants to stand in the way of activities that are harmful to public interests. This might be easier said than done, but it is something that has to be acknowledged and pursued. It is a process, and it is for each one of us individually to make sure that it does not end up being a futile one.

8. From S.E.A.L. to SALE – The Importance of Human-Centric Military Career Transition for Diminishing Integrity Challenges in the Defence and Security Sector and in Society

Valeri Ratchev and Christopher Staudt

Every year, thousands of volunteer soldiers, non-commissioned officers, and officers leave the army after their contracts and return to civilian life with their families. Military and especially war-veterans form a specific social group unlike any other. Their transition from 'uniformed' to 'civilian' life is a period during which they make essential (even vital) decisions regarding personal destiny, psychological health, family life, social perspectives, children, and other dependents' future. Many have overt or covert post-traumatic stress or injuries from combat missions and other critical situations.

Veterans form many valuable qualities and skills, but they must adapt to a specific social and business environment in a relatively short period. The longer their military careers have been, the more civilian life deficits have accumulated. 'Transition' is a process of movement across military, civilian, and business institutional settings, not a single act. It begins while still in service, intensifies during the last period before separation and the first civilian months, and gradually converts into 'reintegration' into society.[1]

Military Career Transition Briefly

The *politics* of veterans' affairs bridge defence and security with the overall government's social, labour, and economic policy. An important lesson reflects this dualism from the democratic experience: *comprehensive support and unique privileges for veterans may positively affect the military profession's attractiveness;* however, *they should be balanced with a societal sense of equity and civility.*

Military Career Transition[2] (MCT) is an outcome-driven process through which military servants and their immediate family members receive government and societal support for transitioning to civilian life. Outcome orientation might be influenced by various political, social, economic, and security circumstances and require an active role from both military in their last year of service and veterans. Castro et al. (2015) break down transition based on four essential factors that connect transition and well-being outcomes:

- *Individual characteristics:* pre-service education and family environment; military service performance; combat and other high-risk experience, type of military discharge, personal military identity and culture, self-perception, and others.
- *Institutional transition management:* performed by the leading institution in collaboration with the armed forces and other ministries, resources for transition allocation, established programmes and benefits packages, available information, advice, and counselling.
- *Public recognition and social support:* respect for the military and recognition of veterans, public support for veterans' care and benefits, CSOs and charities support, responsible business, family, and colleagues' support.

[1] Chris A. Elnitsky, M. Paige Fisher, and Christine L. Blevins, "Military Service Member and Veteran Reintegration: A Conceptual Analysis, Unified Definition, and Key Domains," *Frontiers in Psychology* 8 (2017): 369, https://doi.org/10.3389/fpsyg.2017.00369.

[2] NATO uses this term. Other terms with similar meanings are 'military social adaptation,' 'military resettlement,' 'veterans' affairs,' 'Armed Forces Covenant,' and others.

- *Civilian community support:* local community respect and engagement, local resources mobilized to support militaries' transition.[3]

Countries look at the military career transition system in different ways. Elements to be taken into account include norms, organizations, eligibility for support criteria, procedures, capabilities, and resources. A veteran support system requires an overarching triple objective:

1. To strengthen the military personnel life cycle management of recruitment, retention, transition, and post-service life;
2. To minimize the physical, psychological, spiritual, and social harm experienced by service members and their families as a result of breaches of deeply held moral beliefs. To provide society and business with healthy, skilful, and motivated veterans and family members.]

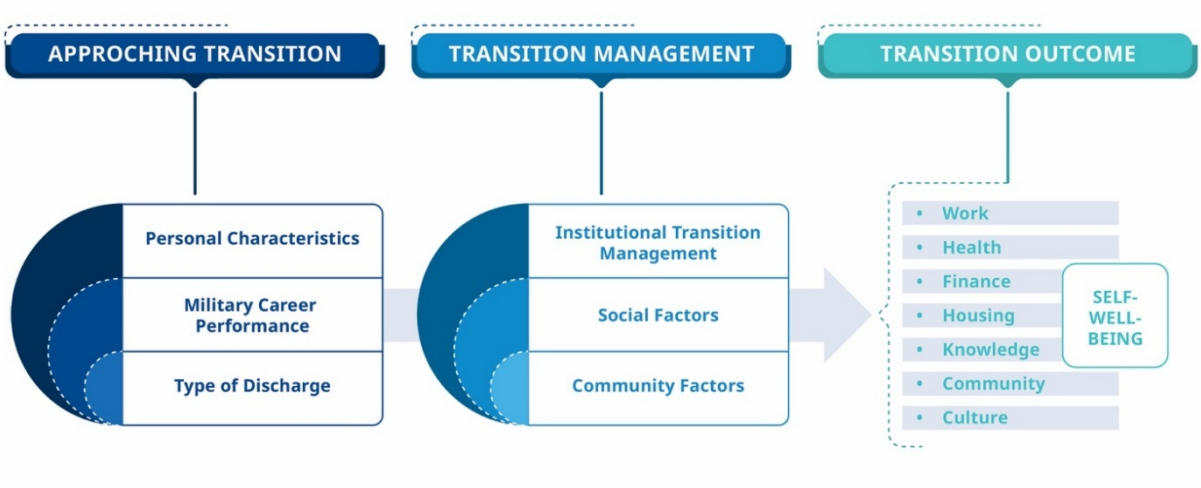


Figure 8.1. Military-to-civilian transition concept.[4]

Box 8.1. Typical "Good Practices" in Building a Military Career Transition System

Pedlar et al. (2019) presented a list of typical features of various frameworks, several of which might be considered 'good practice' for MCT,[5] for instance:

- The diminished well-being that is commonly experienced by releasing members can be mitigated with policies, programs, and services throughout the life course, meaning before release, during service, and during MCT.
- It is essential for serving military members to begin preparing for their MCT well before release.
- There are roles for the whole community in promoting good well-being during MCT, including the transitioning member, their family, the military, veterans' administrations, other government agencies, non-governmental agencies, the private sector, and their communities.
- Transition requires coordination among policy and service actors.'[6]

[5] David Pedlar, James M. Thompson, and Carl Andrew Castro, "Military-to-civilian transition theories and frameworks," in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*, edited by Carl Andrew Castro and Sanela Dursun (London: Academic Press, 2019), pp. 21-50, https://doi.org/10.1016/B978-0-12-815312-3.00003-6.

The transition process is successful when the veterans achieve and maintain a stable level of psychological, physical, and social well-being and can meet their immediate and long-term financial needs. Veterans have committed to a post-military civilian identity and roles that allow them to be well-employed and socially connected according to individual goals and abilities.

An effective and sustainable MCT system is a severe challenge for any country irrespective of the size of the armed forces. Psychological harm and moral injury might be caused by a sense of betrayal including during the MCT process, in the sense that the service member who served his or her country reasonably expects to be assisted in this process. Therefore, it is not merely a matter of choice; it is a fundamental imperative for both modern military and democratic societies. The resources needed for MCT programmes are much less than the damage done by no assistance.

Risks and Remedies in Military Career Transition Areas

As Figure 8.1. illustrates, military career transition amalgamates various political, policy, management, and psychological conditions and influences. The military Human Resource Management (HRM) works alongside governmental, private, or societal retraining, support, and care institutions within the MCT framework. They complement each other with resources and operations to provide better coverage and quality services to veterans and their families. However, they all operate in different organizational and bureaucratic environments, using specific ethical and professional drivers and standards, and coping with diverse challenges. Each military career transition component might be infected by specific corruption, fraud, and bribery viruses that become, in turn, serious defence, political, and societal problems.

The MCT model in a broader civil-military relations context

When turned into government policy, the principal element of 'transition from military service to civilian life' is the definition of 'veteran.' Nations '… recognize the sacrifices that the men and women of the armed forces give to their country and provide care and support for them and their families once they leave the military as veterans.'[7] There are three distinguished models that interpret MCT problems in an exclusive, inclusive, and hard-separation manner. They contain various integrity risks that affect not only those leaving the military but society more generally.

The exclusive approach highlights the logical connection between the military service and combat mission burdens, taken exclusively by servicemen and women, and an understanding that, therefore, *they deserve a different form of compensation from other citizens*.[8] According to Jessica Adler (Smith et al., 2019), veterans understood themselves *as entitled* to government services, and they did not see the veterans' support as charity or welfare but as *earned benefits*.[9] This turns veterans into a particular interest group vying for government-funding privileges. The integrity risk in this model is in the assumption that those who get specific privileges and bonuses during active service will probably enjoy comprehensive veterans' support. However, because the military services and branches do not share equal levels of peacetime operational engagement, this unevenness risks creating internal divisions that could undermine the armed forces' integrity. Further, such military

[4] Adapted from Castro et al., *The State*.

[5] David Pedlar, James M. Thompson, and Carl Andrew Castro, "Military-to-civilian transition theories and frameworks," in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*, edited by Carl Andrew Castro and Sanela Dursun (London: Academic Press, 2019), pp. 21-50, https://doi.org/10.1016/B978-0-12-815312-3.00003-6.

[6] Pedlar, Thompson, and Castro, "Military-to-Civilian Transition Theories and Frameworks."

[7] Christopher Dandeker, Simon Wessely, Amy Iversen, and John Ross, "What's in a Name? Defining and Caring for "Veterans": The United Kingdom in International Perspective," *Armed Forces & Society* 32, no. 2 (2006): 161-177, https://doi.org/10.1177/0095327X05279177.

[8] Herbert Obinger, Klaus Petersen, and Peter Starke, *Warfare and welfare: Military conflict and welfare state development in western countries* (Oxford: Oxford University Press, 2018), 10.1093/oso/9780198779599.001.0001. Full text requested from https://www.researchgate.net/publication/330079687WarfareandwelfareMilitaryconflictandwelfarestatedevelopmentinwesterncountries.

[9] Susan L. Smith, Jessica L. Adler, "Burdens of War: Creating the United States Veterans Health System," *The American Historical Review* 124, no. 1 (2019): 273-274, https://doi.org/10.1093/ahr/rhy541.

exclusiveness can contribute to building 'privilege-based'" societies, as the example could spread to other sectors and professions.

In the alternative 'citizen in uniform' approach, society and military bodies receive equal treatment: there is no emphasis on the military securing society's survival. The 'citizen in uniform' is a *mission statement* that guides the building of the soldiers' self-image. It suggests that citizens' rights and duties somehow continue whilst they serve in the military of a democratic state.[10] The concept does not neglect military service specifics and related restraints on some human rights and citizen freedoms. Instead, it promotes a *positivist (pro-rights) approach* when deciding about legally defined limitations. The presumption is that both parties will benefit more from societal cohesion than exclusive treatment based on specific roles and experience. In this case, veterans would not always like to be dependent on the State and often prefer treatment as simple citizens.

*'*Thank you for the military service and goodbye (in civilian life)' is a military HRM model in which the defence institution completely self-insulates from the veterans' transition to civilian life. It is based on a worldview that states the Ministry of Defence is neither a welfare agency, nor a real estate company, nor a training institution for civilian jobs, nor an employment agency. The Ministry of Defence's job is to build up armed forces that can fight and win wars and perform other military missions. In the moment of separation, the 'military door' is slammed shut and the individual veteran is left to deal with his or her transition. In such cases, military HRM is fragmented and incomplete and creates a dual integrity risk. On the one hand, the military servant is pushed while serving to think about the professional performance and the time when he/she will step back into civilian life. A division in attention can lead to ethical problems when a serviceman is faced with a corruption opportunity – a typical case for those whose position involves allocating significant resources, especially during missions abroad. On the other hand, veterans, without relevant civilian life skills and with massive health, financial, and employment problems, may become a highly vulnerable social group. People with combat training may fall into organized crime networks due to their inability to cope with the realities of civilian life and provide a dignified life for themselves and their families.

All outgoing military personnel should be offered a transition programme relevant to their length of service, professional and personal abilities, labour market trends and service members' aspirations regarding post-military life. Such programmes are necessary to attract and retain high potential qualified personnel. Military Service members who successfully transition to civilian life will spread their stories and generate additional public trust and confidence in the defence and security establishments, the fundamental determinants of the recruitment and retention capacity.

MCT is an essential military HRM component

The effectiveness of the military career transition requires being trustworthy and harmonized with other critical areas of military human resource policy and management. Personnel who are less likely to serve full careers and are to be reintegrated back into civilian life will be subject to a more painful transition than those who have been capitalizing on their high potential successfully acquiring a skillset that adapts easily to civilian life. The MCT is an integral part of overall HRM, and the quality of the transition process can be hampered by a lack of transparency, integrity, and accountability in interrelated areas such as human resources planning, recruitment, performance management, professional development, career planning, retention and pension and compensation (remuneration). Without MCT, two previous stages of the recruitment-retention-transition nexus become incomplete. Thus, there are not the essential incentives that would link personal and organizational interests and neutralize uncertainty for the future.

[10] Peter Rowe, "The soldier as a citizen in uniform: a reappraisal," *New Zealand Armed Forces Law Review* 7 (2007): 1-17, https://natlib.govt.nz/records/21457915?search%5Bi%5D%5Bprimary_collection%5D=findNZarticles&search%5Bi%5D%5Bsubject_text%5D=Soldiers&search%5Bpath%5D=items.



Figure 8.2. MCT in the military human resource management framework.
Source: Gunashvili, David. *Military Competency/Talent (MCT) in the Military Human Resource Management Framework.* Tbilisi: David Aghmashenebeli National Defence Academy of Georgia

Developing and offering the appropriate military care and compensation packages — including wages, health care, reenlistment bonuses, retirement, leave, dependent benefits, and survivor benefits — is necessary for attracting and retaining active duty and reserve personnel with essential skills. It is hardly necessary to mention that salary is only one factor (of many) in the decision to remain in the military: numerous factors affect the decision of individuals to remain in the organization when their initial obligation is completed. The remuneration package highlights how it motivates military personnel to join and stay in the Armed Forces, and chief among these are career and promotion prospects and family issues.

The main integrity risks come down to the limited transparency and accountability of the overall military human resources policy. They might be grounded in some ineffective HRM decisions:

- Shrouded in secrecy, military HRM promotes unethical behaviour along the military chain of command, most often expressed in selective awards, promotions, and punishment to create personality-based networking. The lack of transparency and accountability produces ineffective and inefficient personnel policy and is devastating for combat capabilities. eroding professionalism and service loyalty. In such an environment, honestly serving service men and women feel helpless and discouraged.

- Typical ineffective HRM practices include unclear career paths; frequent and ill-justified changes, vague criteria for promotion; non-transparent career decision-making, non-existence of objective promotion boards, or boards that are easily influenced by high ranked military or civilian authorities seeking to promote their favoured candidates; payment by position and salary scams; uncontrolled premium bonuses often based on secret orders; and the existence of 'ghost' workers and soldiers.

Without any question, military HRM must be conducted based on transparency, accountability, and integrity. Building a merit-based and fair system for producing optimal HR policies should be empowered with effective civilian democratic control over the implementation of these policies by each state organ with military formation, conducted in line with the country's essential security needs and requirements set by the government (strategic military human resource management).

Organizing for effective MCT support

The military career transition is a multi-stakeholder policy sector. Governments designate a leading agency to coordinate policy, programmes, projects, and operations. This agency is also responsible for planning, programming, budgeting, conducting day-to-day activities, and drafting, coordinating, and promoting relevant legal initiatives. Depending on the veterans' affairs model, countries use one of three organizational models for providing MCT support.

- *Ministry of Defence-based MCT support system*. The MoD is responsible for supporting veterans during the transition, playing the role of hub between various departments that provide healthcare, retraining, social, and employment services and support. The essential advantage of this model is that the defence institution may successfully close the 'recruitment-retention-transition' loop in which the components reinforce each other. The MCT process starts within the military units and ends in civilian communities without a break. Therefore, to strengthen the military ethos, it is important that active-duty military personnel care for former service members. The Ministry of Defence-based MCT support system is better protected from corruption because it is based on the military ethos and performance standards.

- *Ministry of veterans affairs-based support*. Establishing a particular governmental department for dealing with military veterans is grounded on the presumption that the MoD is not about social issues and should focus on armed forces capabilities. The model is costly as the department manages healthcare capacities and retraining centres across the country. As it is more or less a bureaucratic system, its effectiveness is questionable and is prone to corruption.
- *Ministry of social affairs-based system*. As the issue is about a new career (employment, business), the model could be based on a traditional governmental employment agency. However, going to another institution for transition assistance, the veteran will turn into 'one of many' – unknown to anybody and not knowing anybody. From an integrity perspective, this model compromises the military HRM loop and puts veterans at an extreme disadvantage at the beginning of their transition to civilian life.

The policymaking divide between administration and implementation is fundamental to building an effective and accountable public policy system protected against politicization and corruption. In some countries, the same veterans' institutions are responsible for setting out and implementing policy. This is done by a specialized veterans' institution (Canada, the U.S.) or the defence department (Australia, Bulgaria). Policymaking and inter-agency coordination are separated from administration and implementation in France, New Zealand, the Netherlands, the UK, and others. In the case where veterans' institutions have policies, the countries believe centralization fits better with resourcing, prioritizing, and implementation control. However, this makes the institutions too large and expensive, with heavy procedures and limited flexibility. In the case where veterans' institutions do not do policies, central administration is smaller, well fitted within the government, focused on veteran politics and policy setting, and downstream coordination, control, and feedback. There is not a universal

solution. The OECD emphasized that separating policy from implementation may help avoid conflicts of interest, such as a policy designed to suit the administrator's needs, not the clients.[11]

Setting out proper eligibility criteria for transition support

The setting out of eligibility criteria for transition support reflects the veterans' affairs model. It begs the question of whether veterans should be thought of as one group or several sub-groups according to eligibility for support and benefits criteria.

The easier way to determine eligibility for assistance is to use an exclusionary method. NATO and European countries use as a benchmark the exclusion from assistance of ex-servicemen and women whose contract has been cancelled after military disciplinary or court sanctions. For that purpose, NATO uses the term 'expulsion' as 'a mandatory discharge, initiated by the organizations based on legal/disciplinary factors.'[12] In this case, the deprivation from transition assistance is intended to strengthen the impact of the disciplinary or legal sanction, making the message very clear, 'the nation will pay money as transition benefit of the military only if they serve honestly, selflessly and effectively.'

For other veterans the criteria for eligibility break down into three primary groups:

- According to the duration of service of different military categories and their families;
- Injured veteran while on duty and their families;
- Families of those who died during a military mission.

Determining the criteria for eligibility for assistance based on the duration of service is a country-specific issue. It very much depends on how the life cycle of the concrete military career is determined by law, and particularly on the system of contracting used for different categories of the military: enlisted, NCOs, and officers, and active and reserve; maximum duration of service as actual calendar years and as an age; admissible years in one rank; and other factors. The enlisted leave the service mainly after filling their temporary contracts, while second in row are those who leave because they are unhappy in the military, and the third in numbers are usually those that fail to meet training criteria.

The definition of eligibility for MCT support is a crucial integrity factor. When set appropriately, the criteria distinguish between war veterans and peacetime military leaders, provide the servants with a clear career perspective based on professionalism and merits performance, set out standards of behaviour, and give families confidence that they will never be abandoned. However, there are significant integrity risks from improperly defined eligibility criteria that may harm armed forces and society:

- *The eligibility criteria matrix is made too comprehensive without relevant implementation resources*. Some countries make the number of those eligible for support large to recognize their role in defending the nation during wars (Croatia, Ukraine). In contrast, others use the method to make peacetime voluntary military service more attractive (the U.S., the UK). Corruption risks escalate when there is a lack of sufficient funding. The choice of who gets support and benefits becomes a corruption tool in the hands of process administrators. In the long queues, the waiting veterans become discouraged and dissatisfied with the executive, the military, and society. The rumour that with corruption, they are getting services and bonuses reaches the active military, the media, and society, creating a negative attitude towards the veterans' affairs policies.

[11] Organisation for Economic Co-operation and Development, (OECD), *The Governance of Regulators* (Paris: OECD Publishing, 2014), https://www.oecd-ilibrary.org/governance/the-governance-of-regulators_9789264209015-en.

[12] NATO Research and Technology Organization, *NATO Human Resources (Manpower) Management* (2012), p. 10, https://apps.dtic.mil/sti/tr/pdf/ADA560294.pdf.

- *Eligibility for support criteria does not recognize military service quality*. The dual requirement for the MCT is to be both universal and fair. Universal means that rank and position do not matter when a serviceman or woman has received a wound in combat, duty, or combat training. Fair means the duration and quality of military service are precisely reflected in support and care criteria eligibility. Everyone who served honestly should get support for transition, but its scope depends on service quality. Failure to balance universality with fairness generates an integrity risk with military service becoming a source of social benefits, with members of the armed forces avoiding any dangerous activity, operation, or mission.

- *The MCT eligibility criteria create lines of division throughout the armed forces*. To encourage participation in peacetime missions, some countries have expanded the definition of 'war veteran' and provided, for example, MCT support to those who have participated in peacekeeping operations as combatants. The problem is that these tend to be army and special forces service members and are very rarely from the air force or air defence. Thus, some soldiers and officers participate in six-eight career missions. In contrast, others do not have any, which is reflected in the package of care and support during their separation from the military.

Providing timely and effective military career transition support and care

Countries employ functional or goal-oriented MCT policy. The former is organized along with the government agencies' missions and functions regarding transitioning militaries. This approach focuses on the agencies' performance and not so much on the effects on ex-militaries and their families. The latter model is based on the accumulated effect of supporting measures and benefits on the overall veterans' well-being. However, in both cases, several elements of support are offered. A comprehensive study[13] on military-to-civilian transition policies, processes, and programme efforts draws a picture of the support provided by NATO member countries (Table 1).

Table 8.1. Elements of support offered by all, most, or some NATO members[14]

All NATO members	Most NATO members	Some NATO members
● Counselling ● Educational assistance ● Employment assistance ● Disability compensation	● Physical health ● Mental health ● Substance abuse	● Home care ● Housing ● Caregiver support ● Transportation support ● Legal services ● Financial support, financial benefits, and financial services

Source: Fossey et al. 2019, p. 53.

Generally, the MCT is organized into three clusters: medical care, military career transition assistance, and benefits.

The cluster 'medical care' provides rehabilitation and health care programmes and assistance.[15] In most cases, veterans and their families have access to military hospitals, sanatoria, and recreation centres when they are present and access the public health care system as ordinary citizens. However, a NATO study estimates that 'the process of transitioning is often more complex for those leaving the military for medical reasons than for those

[13] Matt Fossey, Raun Lazier, Neil Lewis, Nathan Williamson, and Nick Caddick, "Military-to-civilian transition policies, processes, and program efforts," in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*, ed. Carl Andrew Castro and Sunela Dursun, pp.51-74 (London: Academic Press, 2019).
[14] It is important to note that the countries provide various additional services and benefits, such as public health care or old age security, not listed in the table.
[15] Additionally, to what veterans can receive as citizens.

leaving for other reasons.'[16]

The primary integrity risk of medical services is either due to irresponsible and bureaucratic attitudes toward veterans and their family members or direct corruption and bribery for receiving preferred treatment, additional procedures, luxury rehabilitation conditions, medical treatment abroad in more advanced countries, and others. In medical institutions, a major corruption risk comes from costly medicines and procedures being recorded as provided, even when patients never actually receive them.

Box 8.2. Health Care Provided to U.S. Eligible Veterans

The Veterans Health Administration (VA) is the U.S.' largest integrated health care system, with more than 1,200 care sites, and it is consistently ranked among the nation's top health care providers of the following services:

- 'All enrolled veterans have access to VA's comprehensive medical benefits package, including preventive, primary, and specialty care; prescriptions; mental health care; home health care; geriatrics and extended care; medical equipment and prosthetics; and more.
- Most veterans qualify for cost-free health care services, although some veterans must pay modest copays for health care or prescriptions.
- Female veterans can receive primary care, breast and cervical cancer screenings, prenatal care, maternity care coverage, and other gender-specific services.
- Eligible veterans — and their family members — may visit VA's many community-based Vet Centers, which provide no-cost counselling, outreach, and referral services to help the whole family adjust to life after deployment.
- Combat veterans who were discharged or released from active service on or after Jan. 28, 2003, are eligible to enrol in the VA healthcare system for five years from their discharge or release, regardless of their disability claim status. Combat veterans who enrol with VA under this enhanced combat veteran authority will continue to be enrolled after their enhanced eligibility period, although their enrolment priority group may change. Many combat veterans applying after their five-year special enrolment period ends are eligible for enrolment and are encouraged to learn more about these and other health care benefits on VA's health benefits page.
- Access your health care conveniently through digital tools like the My HealtheVet portal, mobile apps, and telehealth services. Secure messaging, digital appointment management, prescription refills and virtual appointments make it easy to connect with us.'

Source: U.S. Department of Veterans Affairs, "VA Health Care," https://choose.va.gov/health?utm_source=google&utm_medium=cpc&utm_campaign=ar_chooseva_enrollment_fy22_targeted military_part1&utm_content=choosevagov&gclid=CjwKCAjwur-SBhB6EiwA5sKtjnlbvfZNoLGnq39oG_Q7St6DgCOz70jVDjdPvRnuWwF8XpHjM6DyJxoClssQAvD_BwE (accessed February 23, 2026).

[16] NATO Science and Technology Organization, *The Transition of Military Veterans from Active Service to Civilian Life* (2021), https://doi.org/10.14339/STO-TR-HFM-263, downloaded from https://www.sto.nato.int (accessed February 23, 2026).

Box 8.3. The UK Strategy for Veterans 2018–2028

Looking ahead, the UK Government intends to deliver public services to veterans across the UK. By 2028, the Strategy aims to make sure that every veteran feels even more valued, supported and empowered and will never be disadvantaged due to their service.

	CROSS-CUTTING FACTORS	
1	Collaboration between organizations	Improved collaboration between organizations offers veterans coherent support.
2	Coordination of veterans' services	The coordination of veterans' provision delivers consistent aims and principles over time and throughout the UK, ensuring veterans, their families and the bereaved are treated fairly compared to the local population.
3	Data on the veteran community	Enhanced collection, use and analysis of data across the public, priva and charitable sectors to build an evidence base to effectively identif and address the needs of veterans.
4	Public perception and understanding	The UK population value veterans and understand their diverse experiences and culture.
5	Recognition of veterans	Veterans feel that their service and experience are recognized and valued by society.
	KEY THEMES	
1	Community and relationships	Veterans are able to build healthy relationships and integrate into their communities.
2	Employment, education and skills	Veterans enter appropriate employment and can continue to enhanc their careers throughout their working lives.
3	Finance and debt	Veterans leave the Armed Forces with sufficient financial education, awareness and skills to be financially self-supporting and resilient.
4	Health and well-being	All veterans enjoy a state of positive physical and mental health and well-being, enabling them to contribute to wider aspects of society.
5	Making a home in civilian society	Veterans have a secure place to live either through buying, renting o social housing.
6	Veterans and the law	Veterans leave the Armed Forces with the resilience[17] and awareness to remain law-abiding civilians.

Source: UK Ministry Defence, *The Strategy for Our Veterans. Valued, Contributed, Supported*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755915/Strategy_for_our_Veterans_FINAL_08.11.18_WEB.pdf.

[17] Resilience is defined by NATO as 'The individual and collective capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions, and to ensure the continuity of the Alliance's activities.' (Source: North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," last updated November 13, 2024, https://www.nato.int/cps/en/natohq/topics_132722.htm).

The cluster 'military career transition assistance' is organized generally into three phases: 1) orientation, consulting, and individual planning; 2) personalized vocational training; and 3) assistance for civilian employment or business development. Assistance is provided exclusively to those Service leavers that are still of working age. In the countries without special veterans' affairs institutions, phases 1 and 2 are usually performed by defence ministries. At the same time, employment or business development assistance is offered either by the departments of social policy and labour structures or by businesses or charities under contract with the MoD. In countries with established veterans' affairs governmental agencies, these agencies lead the process in collaboration with defence and social policy institutions, using private contractors.

The riskiest aspect is the relationships between assistance programmes managers and retraining and re-employment providers from an integrity perspective. Demanding and receiving bribes from for-profit schools, training centres, and consultancy companies in exchange for enrolling military veterans (especially disabled) and family members may devastate overall MCT policy.

The cluster 'benefits' includes various programmes for financial assistance. Compensation schemes are established for supporting personnel injured because of their service, including life-long assistance in case of permanent impairment. Financial benefits include lump-sum payment, tax relief, guaranteed income payment, emergency financial support, compensations for eligible prisoners of war, death and bereavement compensation, survivor's pension, burial assistance, grave marker maintenance, and support for payment of non-service-related medical costs, and others. The veterans' organizations are also eligible for state support through grants, public-private partnerships, and contracting mechanisms, an undeniable element of both state's support to self-organized veterans and the development of a vibrant national civil society.

However, the benefits policy as part of MCT is more complex than the other clusters. Determined superficially without in-depth social and psychological analyses in society and among the military might create significant division lines within societies, especially those that have suffered defensive wars (e.g. Croatia, Ukraine). The provision of benefits requires a long delivery chain with institutional, regional, community, and corporative engagements that are difficult to control and keep accountable. Unfair service to veterans in rural areas is also a possible ethical challenge.

Applying Good Practices for Making MCT Effective and Honest

Research into good practices, undertaken by authors and organizations, provides a holistic picture of the interior and immediate features of the military transition to civilian life. Good practices are found across the chain of politics-policy-programmes-actions nexus. However, despite the significant achievements and ongoing developments, even the most advanced countries consider that the veterans' care and benefits system requires continued improvement and, in some cases, serious reforms. Notwithstanding that the countries have different visions about the 'ideal' veterans' policy, some practices might be considered principles of effectiveness and integrity:

Box 8.4. Good Practices in Providing Effective and Honest Military Career Transition

The introduction of the MCT function stimulates the build-up of solid institutional preconditions. Anyone going through military service, no matter their overall career progress, will become a positive ambassador of military service and one of the essential builders of trust and gainers of the support of society. The search for better ways to serve veterans reflects the specific context in which governments established veterans' policy.

a. The policy must advance the interests of veterans and their families, society, and economy in a balanced manner. Nothing is more important than the definition of 'veteran' as it defines policy scope, cost, and effectiveness. Both inclusive and exclusive definitions have advantages and disadvantages from the perspectives of veterans, society, armed forces, and the economy.

b. Veterans' policy should not lead to isolating veterans from society. Rather the authorities should provide care and benefits as much as possible through societal instruments, resources, and actors. It should be connected precisely to relevant national policies such as welfare, social insurance, disabilities, gender equality, and many others.

c. A proper socio-political definition of a successful military transition provides the cohesion, support, and sustainability of veterans' policy. As a policy objective and measurable benchmark, the definition has implications for policy design, transparency, and accountability. It helps build a shared understanding of who is responsible for what and what collaboration and contribution are expected from each stakeholder. Moving from veterans' policy services and products towards veterans' wellbeing (wellness) is the most advanced and challenging good practice.

d. The policy, institutions, and delivery system must be veteran-centric. Veterans and their families are at the heart of policy design, the organization of leading institutions, and implementation programmes. The essence of suitable arrangements for veterans' policy is a horizontal collaboration with clearly defined responsibilities and accountability.

e. Policy implementation is made as public-private, veterans-owned, and community-based as possible. Veterans' organizations should play an essential role in the system.

f. Strategic communications must make sure that veterans have precise information to make informed decisions and that they have easy access to the service delivery system.

The MCT system is prone to corruption, bribery, and unethical treatment of veterans. Transparency, public-private division of labour, and accountability should be established strictly along with the policymaking and service delivery chain.

a. Transparency should be provided for all direct and indirect services and benefits envisaged by laws and other sub-law institutional documents. However, the transparency of service delivery procedures, essential outcomes from veterans' perspective, and cost-effectiveness ratios are no less important. Transparency must not be an issue of choice but legally defined at all levels.

b. Engagement of societal actors, especially the veterans' family members and organizations, is critical for the MCT effectiveness, cohesion, and fairness. Establishing government-societal checks and balances within the MCT service delivery system is an essential instrument of corruption prevention.

c. Accountability must be secured for all actors engaged — governmental, public, or private. Accountability should reflect the procedures of service and benefits delivery and the outcomes and effects on veterans and their families.

Case Study: NATO's Military Career Transition Programme under BI principles in Ukraine

Since its independence, Ukraine has had a unique experience and tremendous challenges in coping with problems of veterans, massive discharge of personnel, and military service leavers. The absence of MCT weakened the integrity, transparency, and accountability of HRM decisions and put the defence and security sector at risk. The policy of military career transition, as well as societal attitudes towards it, are indicative of the maturity of the Ukrainian civil-military relations. Crucially, it is an element of strategic importance as Ukraine

confronts a direct military crisis.

Russia's aggression in 2014 has turned the veteran problem into a severe political and social issue and a critical factor in national security. By February 2022, approximately 1.2 million veterans were registered. In response to the Russian military intervention, NATO has reinforced its support for capability development and capacity building in Ukraine. At the Wales summit (2014), a decision was taken to launch six trust funds, one of which is the Military Career Transition Trust Fund (MCT TF). Since the Warsaw Summit (2016), NATO's practical support to Ukraine has been included in the Comprehensive Assistance Package (CAP) for Ukraine, guaranteeing NATO's contribution for MCT TF objectives as part of the Ukrainian defence and security sector cooperation.

In 2021 the Ministry for Veterans Affairs of Ukraine (established in 2018) was, for the first time, incorporated into NATO's Planning and Review Process. Here is a clear political sign that structured and systematized professional military service leaver post service assistance and veterans' well-being and reintegration into civilian Ukrainian society is of the utmost importance for the promotion of security, stability and resilience. The new Partnership Goal for MCT and Social Provision enhances the Ministry for Veterans Affairs' structured approach in the transformation and modernization efforts based on NATO's BI principles.

The objective of the NATO-Ukraine Military Career Transition Programme is to develop and implement a sustainable, effective, and integrated approach to the resettlement of military personnel in the Ukrainian Armed Forces, the National Guard and the State Border Guard Service. NATO supported the Ministry for Veterans Affairs (MVA) of Ukraine in 2020 and 2021 with several projects, jointly implemented with the MVA staff and specialized civil society organizations. A 'White Book' comprised: European Union member states' veterans' policies and good practices analysis; a feasibility study of the Ministry's veteran-centric service delivery model; and a set of principles for establishing a reform-managing Project Office that combined may develop the MVA as an influential and integral veteran-centric institution. The NATO MCT Programme also provided support to the Ministry's regional staff, setting guidance on the psychological handling of post-concussion syndrome and related war veteran conditions, creating facilitation tools and capacities for efficient cooperation between the Ministry and dedicated NGOs.

A joint development programme until 2025 provided support to the inter-ministerial working group to implement the MCT's resettlement structure based along three lines. The provision of 1st Line MCT support is the responsibility of the commanders at the unit level and will be limited to informative and administrative support. The principal task of the 2nd Line is to provide advice and guidance on the MCT package (benefits) that will best suit service leavers (individually tailored resettlement plan). MCT support at the 3rd Line with the labour market trajectory will be provided by the already existing and specialized State Employment Centre and its regional subsidiaries.

According to Ukraine's Pension Fund, as of 1 January 2025, there were 365,999 registered war veterans, including more than 121,000 veterans with disabilities. The MVA predicts that after the war, the number of veterans, together with their family members, could reach 5 to 6 million people, or roughly one in every six Ukrainians. Now, thousands of service members return to civilian life, facing discrimination, discouragement and the need to renew or completely change their professions.[18]

The NATO experience in Ukraine illustrates that the military transition back to civilian life is a strategic issue. Certainly, it has a multi-dimensional impact on combat readiness, societal support for respected military men and women, and business development. The ongoing crisis will inevitably escalate the overall value of MCT.

Conclusion

The policy for veterans' reintegration into society benefits all citizens and the State. Caring for veterans is society's moral duty to those who risk their lives to protect them. This, in turn, mitigates the risk of moral injury. Still, it is an essential contribution to social cohesion, to its consolidation around the highest national moral

[18] UkraineWorld. 2025. "One Step Toward Reintegration: Ukraine's Veterans on the Path to New Careers." October 9, 2025. https://ukraineworld.org/en/articles/opinions/one-step-toward-reintegration-ukraines-veterans-new-careers

values and strengthening the sense of national identity. Good practices show something fundamental, for veterans, their civilian social environment is more critical than their privileges.

Veterans are an asset to strengthen local communities and economy. Veterans posses unique capabilities and skills that may provide local communities with reliable support, especially in emergency and high-risk cases. The economy may receive 'free of charge' experienced and skilful empowerment through the veterans' retraining and specialization courses and education benefits.

Socially secured, employed, and honoured veterans are the surest incentives for sustaining capable armed forces and national security. The whole-of-government care for a successful military-to-civilian transition affects the armed forces' ability to recruit and retain talented people to serve longer. Veteran policy is closing the loop of military human resource policy and management in a manner that is moral and rational.

The essence of MCT includes respect and care, individual participation and institutional service, and it should also be based, as much as possible, on the principles of the individual approach. However, the process is driven by political, social, and economic considerations. Military career transition reaches beyond defence policy, interlinking defence and social, labour and economic policies. Transparency and the accountability of the 'whole-of-government' approach will secure the MCT system's effectiveness and integrity.

9. Risks: Budgeting and Financial Management

Francisco Cardona

Public expenditure, including in the military, is recognized as a major source of vulnerability to corruption. In many countries, most public spending is channelled through public budgets. Therefore, it is important to foresee and prevent corruption risks early in the budget formation process and in implementing the spending side of the budget.

This chapter deals with corruption risks associated with public expenditure, with a particular focus on military budget allocations. Two practices have been identified as good ones in international discussions. One is a strengthened transparency in budgeting. The other is to build strong financial controls and audits into the public expenditure system. We will give an overview of these two practices in this chapter.

What is Government Budgeting?

According to the OECD SIGMA, a budget is one or more documents that include the plan of the future activities of a government or a governmental organization and how they are to be funded. The budget is generally prepared annually, and comprises a statement of the government's proposed expenditures, revenues, borrowing and other financial transactions in the following year.

The budgeting process consists of reviewing budget requests from ministries and agencies by designated staffers of a central budget department at the finance ministry. There the budget requests are analysed, alternatives are developed, conclusions are reached, and recommendations are made.

These operations lead to the budget formulation by the executive, which contains standardized documentation. The set of budgetary documents presented to a parliament usually is, in addition to proposals relating to government spending, revenues and borrowing, a statement of the economic and financial context for budget proposals, the government's economic policy objectives, medium-term macroeconomic projections, and some explanation of the government programmes and activities to be funded under the budget. A bill is submitted to parliament, and parliament authorizes expenditure by approving either a Budget Act or an Appropriation Act that is consistent with budget proposals.

Budgeting is public financial management (PFM), which encompasses all aspects of public finances and government spending. Budgeting comes between revenue mobiliZation and collection, mainly from taxation, and the actual spending of government funds (on procurement, government services, subventions, and payroll). Budgeting is the planning and approval process. Accounting and auditing of government expenditures (e.g. internal and external controls) come in later.[1]

Budgeting Standards, with Special Reference to Transparency in Defence Budgeting

According to Transparency International,[2] a transparent and detailed budget that is available to the public is key to holding governments accountable to their citizens. Opaque defence spending decisions can promote corruption and hinder the effectiveness and efficiency of military and security forces. Excessive secrecy can lead to higher levels of uncertainty, distrust, and suspicion in a society, but also at a regional and global level. There

[1] For a comprehensive discussion on the budgetary process, including a good glossary, see Barry H. Potter and Jack Diamond, *Guidelines for Public Expenditure Management* (Washington, DC: International Monetary Fund, 1999), https://www.imf.org/external/pubs/ft/expend/index.htm.

[2] Transparency International Defence & Security, "The transparency of national defence budgets," March 10, 2016, https://ti-defence.org/publications/the-transparency-of-national-defence-budgets/.

is a growing awareness that stability and security can be enhanced through increased disclosure of defence-related information.[3] A transparent defence budgeting process can have international benefits.

Several international initiatives promote the transparency of public budgets generally and in the defence area specifically. The following are, in chronological order, worth mentioning:[4]

1. **United Nations:** The 1980 UN *Instrument for Standardized International Reporting of Military Expenditures* within the United Nations Office for Disarmaments Affairs (UNODA) remains the only official worldwide reporting system to date. It is a voluntary instrument for disclosing defence-related expenditures. The original goal of MilEx–to facilitate reduction of military expenditures–gradually gave way to another important goal: to increase transparency and build confidence among states.[5] UN General Assembly resolution 56/14 of December 2001, adopted by acclamation without ballot by member states, observed that transparency in military matters is an essential element for building a climate of trust and confidence among states worldwide.[6] Also, a better flow of objective information on military matters can help relieve international tensions and is, therefore, an important contribution to conflict prevention. The *UN Standardized Reporting Instrument for Military Expenditures* has also played an important role in acting as a model for similar reporting instruments, such as the one used by the Organization for Security and Co-operation in Europe (OSCE). In 2025, 62 states reported their military expenditure, while world military expenditures reached a record high of USD 2.72 trillion in 2024.[7]

2. **OECD**: Drawn up in 1999, the *OECD Best Practices for Budget Transparency* does not provide specific standards for military budgets, probably because this is a matter that has been dealt with at length by UNODA since 1980. However, it provides guidelines for government disclosure of information on public budgets and includes three main components: 1) the main budget documents that governments should disclose with an appropriate content; 2) specific information to be disclosed in those reports including both financial and non-financial data; 3) methods for ensuring that reports are accurate and transparent. The best practice manual is meant to encourage OECD member states to release more comprehensive and accurate fiscal data.[8] Building on this earlier guidance, the OECD introduced the Budget Transparency Toolkit in 2017, which provides practical tools for governments to design, implement, and monitor transparency reforms across the entire budget cycle. The toolkit expands the earlier principles by offering operational guidance on issues such as citizen engagement, oversight institutions, fiscal reporting standards, and the use of budget transparency to strengthen accountability and public trust.[9]

3. **NATO**: Launched in 2004, the *NATO Partnership Action Plan on Defence Institution Building* defines shared objectives and encourages exchange of knowledge. More specifically it does so on issues pertaining to the building of effective and efficient defence institutions which function under proper

[3] Mariya Gorbanova and Leah Wawro, *The Transparency of National Defence Budgets: An Initial Review* (London: Transparency International UK, September 2011), https://www.transparency.ge/sites/default/files/post_attachments/Report%20on%20Defence%20Budget%20Transparency.pdf.

[4] For an extended review of international standards see Geneva Centre for Security Sector Governance (DCAF), *International Standards of Financial Oversight in the Security Sector*, (Geneva: DCAF, 2015), https://www.dcaf.ch/sites/default/files/publications/documents/EN_International_standards.pdf.

[5] United Nations Office for Disarmament Affairs. "Military Expenditure." Accessed March 16, 2026. https://disarmament.unoda.org/en/our-work/cross-cutting-issues/military-confidence-building-measures/military-expenditure

[6] United States Department of State, Bureau of Political-Military Affairs, "United Nations Instrument for Reporting Military Expenditures," April 15, 2002, https://irp.fas.org/news/2002/04/dos041502b.html.

[7] United Nations Secretary-General, *Objective Information on Military Matters, Including Transparency of Military Expenditures: Report of the Secretary-General*, A/80/225 (New York: United Nations General Assembly, July 22, 2025).

[8] Organisation for Economic Co-operation and Development (OECD), *OECD Best Practices for Budget Transparency* (Paris: OECD, 2002), http://www.oecd.org/dataoecd/33/13/1905258.pdf.

[9] OECD. *OECD Budget Transparency Toolkit: Practical Steps for Supporting Openness, Integrity and Accountability in Public Financial Management.* Paris: OECD Publishing, 2017. https://www.oecd.org/publications/oecd-budget-transparency-toolkit-9789264282070-en.htm

democratic and civilian control.[10] Central issues of the plan involve transparent and effective processes of budget allocation for the defence sector with the objective of developing 'effective, transparent and economically viable management of defence spending, taking into account macro-economic affordability and sustainability; develop[ing] methods and policies in order to cope with the socio-economic consequences of defence restructuring'.

The Benefits of Budget Transparency

The benefits of budget transparency, according to the OECD, can be summarized as follows:[11]

- Accountability: Clarity about the use of public funds is necessary so that public representatives and officials can be made accountable for effectiveness and efficiency.
- Integrity: Public spending is vulnerable not only to waste and misuse, but also to fraud and corruption. 'Sunlight is the best policy' for preventing corruption and for maintaining high standards of integrity in the use of public funds.
- Inclusiveness: Budget decisions can profoundly affect the interests and living standards of different people and groups in society; transparency involves an informed and inclusive debate about budget policy impacts.
- Trust: An open and transparent budget process fosters trust in society that people's views and interests are respected, and that public money is spent well.
- Quality: Transparent and inclusive budgeting supports better fiscal outcomes and more responsive, impactful, and equitable public policies.

Assessing the Transparency of Defence Budgeting

The relevant questions to be raised to assess the degree of transparency in defence budgeting have to do with the extent to which governments publish (or do not) their budget proposal, enacted budget and audit reports and the percentage of secret items in these documents. The following are some of the questions that could be asked to assess transparency in budgeting:[12]

- Is the defence budget transparent and does it show all key items of expenditure?
- Is the approved defence budget publicly available?
- Are sources of defence income, such as equipment sales or property disposal, published?
- What percentage of the defence and security budget is dedicated to spending on secret items relating to national security and intelligence services?
- Have there been in recent years serious political attempts to strengthen or conversely to reduce the transparency of defence budgets?
- Have the media, the civil society, international organizations, or others raised concerns in recent years about the transparency of defence, intelligence, or security budgets?

[10] North Atlantic Treaty Organization (NATO), *Partnership Action Plan on Defence Institution Building (PAP-DIB),* June 7, 2004, https://www.nato.int/cps/en/natohq/official_texts_21014.htm (accessed February 23, 2026).
[11] Organisation for Economic Co-operation and Development (OECD), *Quality Budget Institutions: Developments in OECD countries*, (Paris: OECD Publishing, 2025), https://doi.org/10.1787/8e811202-en.
[12] A larger number of questions for assessing budget transparency, financial control and external audits can be found in Svein Eriksen and Francisco Cardona, *Criteria for Good Governance in the Defence Sector: International Standards and Principles* (Oslo: Centre for Integrity in the Defence Sector (CIDS), 2015), pp. 28, https://www.dfo.no/sites/default/files/fagområder/Rapporter/Rapporter-Difi/2015_1_guidance_criteria_for_good_governannce.docx.pdf.

Extrabudgetary Funds and Corruption

Corruption may occur in every stage of the budgeting process. These stages are: 1) long-term planning; 2) annual budget formulation in the executive branch; 3) debate and approval of budget appropriations in parliament; 4) implementation by various ministries and government agencies; and 5) oversight and control (audit) by several institutions.

Ideally, the budget process should allocate public resources in a strategic, transparent, accountable, fair, controllable, and democratic way. However, this is not always the case, as in many nations budgetary allocations are the result of heavy *quid pro quo*, often opaque political negotiations rather than of a rational planning forecast based on needs assessments. Systematic opaque practices often lead to systemic corruption.[13] Not infrequently large funds are allocated *outside* of the budget to the detriment of fiscal transparency.[14]

Extrabudgetary funds are generally understood as government transactions, often with separate banking and institutional arrangements that are not included in the annual state (federal) budget law and the budgets of subnational levels of government.[15] In developed countries, the social security fund is the most typical extrabudgetary fund. The agencification processes in many OECD countries have also led to the creation of extrabudgetary funds in the hands of those government arm's-length agencies, allegedly to increase the margins of their financial manoeuvres. In most EU and OECD member states, the extrabudgetary funds are presented, however, as part of the budget process within a consolidated budget. In less developed countries extrabudgetary funds tend to be less transparent. They usually reflect weaknesses in public financial management systems and may be alien to the notion of consolidated budget. This naturally increases corruption risks.[16]

Extrabudgetary funds are also sometimes associated with: the dilution of accountability and control, problems in reporting and consolidating fiscal data; the diversion of limited administrative capacity; and as potential sources of political and administrative corruption.[17]

One major risk from extrabudgetary funds is their tendency to proliferate into hundreds or thousands of individual units, thus atomizing political governance and fragmenting and undermining the overall quality of public financial management. For example, the significant number of extrabudgetary funds in many central and eastern European countries in the early 1990s, including in Russia, Poland, and Bulgaria, as well as in Türkiye, had a damaging impact on their overall fiscal performance. The current proliferation of extrabudgetary activities through the formation of public law entities and non-commercial organizations poses similar fiscal risks in countries such as Georgia and Armenia. Ghana is another example of a country with a plethora of statutory funds in sectors such as roads, social security, and mining, that have had an adverse impact on overall budget management.[18]

---

[13] Jan Isaksen, "The budget process and corruption," U4 Anti-Corruption Resource Centre, January 1, 2005, https://www.u4.no/publications/the-budget-process-and-corruption.

[14] U.S. Department of State, *2020 Fiscal Transparency Report*, June 15, 2020, https://www.state.gov/2020-fiscal-transparency-report/. This report also indicates the main features and requirements for fiscal transparency in budgeting.

[15] For a comprehensive discussion on the various types of and rationales for extrabudgetary funds, as well as their potential problems, see Richard Allen and Dimitar Radev, *Extrabudgetary Funds* (Washington, DC: International Monetary Fund, June 11, 2010, https://www.imf.org/external/pubs/ft/tnm/2010/tnm1009.pdf.

[16] Richard Allen and Daniel Tommasi, eds., *Managing Public Expenditure: A Reference Book for Transition Countries* (Paris: OECD Publishing, 2001), https://doi.org/10.1787/9789264192607-en.

[17] Ibid.

[18] Allen and Radev, *Extrabudgetary* Funds, 13.

The Need for Black Budgets

Extrabudgetary funds oftentimes function as black budgets or covert public spending, which is true in all democracies. In the United States, black budgets are estimated to be over USD 50 billion a year, taking up nearly 10 percent of the USD 700 billion American defence budget, according to the *Washington Post* in 2013.[19]

Covert spending receives various names depending on countries, which are roughly equivalent from the perspective of their contents and functionality: black budget (United States), *fonds spéciaux* (France*) fondos reservados* (Spain) or 'discretionary funds' (Türkiye).

A black budget or covert appropriation is a government budget that is allocated for classified or secret operations.[20] Amounts allocated to secret operations are classified for security reasons. There are mechanisms in most parliaments to ensure that a limited number of MPs (usually requiring security clearance) receive information about classified budgets. It is important to underline that even if the existence of black budgets cannot be prevented, some safeguards and mechanisms of control are, or should be, in place.

Legal interpretations on the constitutionality of black budget issues must answer many questions such as: are black budgets justified enough? Are security exemptions allowed to remain outside the general financial management transparency rules? What is the justification for that? When does opaqueness become a threat to democracy? What is the acceptable scope and use of black budgets? Covert spending has been conducive to major corruption scandals around the world.

- In France in 2000 there was a public outcry against paying civil servants' salary supplements in opaque ways from the *fonds spéciaux*. The President of the Court of Accounts sent a memo to the Prime Minister asking him to put an end to these sweeping practices and asking for more transparency while urging the reduction of the scope of these *fonds spéciaux*, not least for the sake of the modernization of the public management. The acknowledgment of the need for a part of the budget to be secret was not put into question, as it is a necessity for every democracy to protect internal and external security.[21]

- In Spain, black budgets ('*fondos reservados*' or reserved funds) are regulated by a 1995 Law, as amended several times. They are those so determined by the state budget laws, allocated for expenditures needed for the state defence and security. This spending, as opposed to other public spending, must be kept confidential and is subject to a special system of justification and control. Only the ministries of foreign affairs, defence, interior, and intelligence services may have black budgets. Scandals arose in 2019 because the Ministry of the Interior used the police and its black budget to spy on and disrupt the judicial investigations on corruption of the then ruling party.[22]

The use of black budgets brings to the fore constitutional questions that involve law and public policy as well as public management. There remains an open question of where interpreters of the law must stand when balancing national security concerns, issues of standing, compromising sources and methods, or those who argue the process already possesses internal checks. Finding satisfactory solutions to this problem of the use and

[19]Barton Gellman and Greg Miller, '"Black budget" summary details U.S. spy network's successes, failures and objectives' *The Washington Post*, August 29, 2013, https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (accessed February 23, 2026). See also User28660, 'Does the U.S. military have the means to spend a lot more than the allotted budget for the military?,' *Politics Stack Exchange*, August 13, 2021, https://politics.stackexchange.com/questions/68123/does-the-u-s-military-have-the-means-to-spend-a-lot-more-than-the-allotted-budg (accessed February 23, 2026).

[20] Andrew J. Swab, *Black Budgets: The U.S. Government's Secret Military and Intelligence Expenditures*, Briefing Paper No. 72 (Harvard Law School, May 2019), https://scholar.harvard.edu/files/briefingpapers/files/72_-_swab_-_black_budgets.pdf.

[21] François Logerot "Note à l'attention de Monsieur le Premier ministre relative au régime des fonds spéciaux," Cour des comptes, October 10, 2001, https://www.vie-publique.fr/sites/default/files/rapport/pdf/014000737.pdf; see also *Sénat, Projet de loi de finances pour 2002: Services généraux du Premier ministre, Rapport général no. 87 (2001-2002), tome III, annexe 34*, November 22, 2001, https://www.senat.fr/rap/l01-087-334/l01-087-33417.html.

[22] Nicolas Tomás, "Operation Kitchen: former Spanish interior minister Fernández Díaz accused by judge," *El Nacional*, September 18, 2020, https://www.elnacional.cat/en/politics/spanish-fernandez-diaz-operation-kitchen_539463_102.html (accessed February 23, 2026).

abuse of black budgets is pending in many countries. It remains a pursuit worthy of serious research and practical, sound policy recommendations, which remain, though, elusive.

The Need for a Solid Public Financial Management System

Public Financial Management (PFM) is a central element of a functioning state. It encompasses all government financial activities. The main stages of the PFM cycle are revenue collection, budget preparation, budget execution, accounting and reporting, and audit and oversight. Improving a country's PFM provides extensive and enduring benefits, including stronger institutions, reduced poverty, greater gender equality and balanced growth.[23] Evidence shows that interventions at every stage of the PFM cycle have a positive impact on curbing corruption.[24]

A World Bank report also found a positive correlation between public expenditure and financial accountability (PEFA) scores and perceptions of corruption.[25] One conclusion is that a good system of PFM is indispensable for good democratic governance and for reducing corruption.

Public financial management is not only about applying technical expertise. PFM technical reforms have in fact a limited effect on public sector corruption. These reforms may reduce bureaucratic and petty corruption somewhat, but they will have little impact on political corruption.[26]

Corruption in financial management often includes political corruption, rent seeking, extortion and illegal levies from citizens. In low-transparency environments, such as in the national security spending, financial management often leads to the misappropriation and embezzlement of public funds.

A solid PFM system requires financial control, audits, and/or inspectorates as its main instruments.

Financial Control, Inspectorates, and Internal and External Audits

Examination of the practices of state bodies allows the audit authorities to determine the extent to which they comply with established standards for financial accounting and reporting. These are key mechanisms for ensuring the proper use of public money in terms of its legality, regularity, and propriety (compliance auditing), fair presentations of financial statements (financial auditing) and cost efficiency, and effectiveness (performance auditing). Lack of a proper internal and external audit can lead to misuse of public funds entrusted by citizens to the government's stewardship.

The mechanisms for carrying out financial control in the defence sector vary depending on countries. The most common are the following:

- *Inspectors General*: Inspectors General (IGs) can either have a purely military role, or an auditing, investigation, or other special task. IGs can review processes and mechanisms for improving efficiency and value for money and for producing reports and recommendations for reducing costs, eliminating fraud, reducing waste, investigating the abuse of authority, improving performance, strengthening internal controls, and for achieving compliance with laws, regulations, and policy.

- *Public Internal Financial Control* (PIFC) systems aim to provide adequate and transparent methods for ensuring that public funds are used for the objectives determined by the government and parliament.

[23] Jorum Duri, "The impact of public financial management interventions on corruption," U4 Anti-Corruption Resource Centre, May 4, 2021, https://www.u4.no/publications/the-impact-of-public-financial-management-interventions-on-corruption.
[24] Jorum Duri, "Overview of the impact of PFM interventions on corruption," *H*elpdesk Answer, Transparency International Knowledge Hub, May 27, 2021, https://knowledgehub.transparency.org/helpdesk/overview-of-the-impact-of-pfm-interventions-on-corruption.
[25] World Bank, *Public Financial Management Reforms in Post-Conflict Countries: Synthesis Report* (2012), https://documents1.worldbank.org/curated/en/945231468340162289/pdf/699640WP0P1206070023B0PFM0Web0Final.pdf.
[26] Allen and Tommasi, *Managing Public Expenditure*.

PIFC is preventive in nature and aims to ensure that adequate systems are in place to hinder, as far as possible, the occurrence of corruption and fraud. There are three key components in public internal financial control that are required for achieving efficient and effective use of public money within public agencies: financial management and control; internal auditing; and a central harmonization unit (CHU) for developing methodologies and standards relating to the first two components.

- *External Audit*: External audits have a crucial role in the evaluation of and reporting to parliament on how the financial control and internal audit systems are implemented. External audits provide a key mechanism by which parliaments and taxpayers scrutinize the way in which the government uses the money voted to it and holds governments to account. Throughout the world, national supreme audit institutions (SAIs or Courts of Accounts) have been established with the task of auditing the orderly and efficient use of public funds. SAIs can accomplish their tasks objectively and effectively only if they are independent of the audited entity and are protected against any outside influence.[27] SAIs should be authorized to audit the legality and regularity of financial management, as well as to carry out performance audits. All public financial operations, regardless of whether and how they are reflected in the national budget should be subject to audit by SAIs. If a part of public expenditure is excluded from the budget, it should not be exempted from audit by the SAI.

Special Considerations on the Audit of Secret or Politically Sensitive Subjects

The SIGMA Programme of the OECD[28] noted in 1996 that government agencies which deal with secret or politically sensitive subjects can be expected to try to restrain the information they provide to their auditors because they are afraid of a breach of security or confidentiality by auditors. SIGMA provided some practical recommendations for mitigating this problem.

To improve the willingness of the auditee to provide the auditor with the information he needs the auditor has first to guarantee his auditee will use the information with proper discretion and that the secret or sensitive information will not be released outside the auditor's organization. Depending on the level of secrecy, the auditor must take appropriate measures to safeguard the information from unauthorized access. These measures may include secluded rooms, a specific secret registry, a tapping-proof discussion room and the installation of TEMPEST-proof facilities, copying machines and computers. Furthermore, any auditor involved in classified audit issues must be regularly checked in strict accordance with the applicable regulations to maintain a high standard of personnel security.

In short, to obtain the information he needs the auditor must live up to the same security standards as are applicable to his auditee. This principle applies whether there are secret subjects or merely politically sensitive ones. Restricting the number of staff involved in an audit may, in the extreme, mean only one person auditing the subject. The more people who know about a secret audit issue, the more difficult it is to protect information. Planning an audit of a secret subject therefore also means deciding on the minimum of staff to be involved. Consulting the auditee about this number is in most cases advisable.

Conclusions

1) 'Financial oversight in the security sector is a tool for ensuring that public funds allocated by the state budget for the security of the people are spent in a transparent and accountable manner'.[29]

---

[27] International Organization of Supreme Audit Institutions (INTOSAI), "Audit Standards," https://www.intosai.org/focus-areas/audit-standards (accessed February 23, 2026).
[28] Organisation for Economic Co-operation and Development (OECD), *The Audit of Secret and Politically Sensitive Subjects: Comparative Audit Practices*, SIGMA Papers, No. 7, (Paris: OECD Publishing, 1996), https://doi.org/10.1787/5kml6g916dlw-en.
[29] Nicolas Masson, Lena Andersson, and Mohammed Salah Aldin, *Strengthening Financial Oversight in the Security Sector* (Geneva: DCAF, 2012), https://www.dcaf.ch/sites/default/files/publications/documents/Financial_oversight_English_full.pdf; see also Geneva Center for Security Sector Governance (DCAF), *Financial Oversight in the Security Sector: A Toolkit for Trainers* (December 3, 2015), https://www.dcaf.ch/financial-oversight-security-sector-toolkit-trainers.

2) Transparency in budgeting and effective oversight of financial management in the defence and security sectors are fundamental to building public confidence in those sectors.

3) Budgeting and oversight must aim at ensuring that:[30]

   i. formal (i.e. those with a formal mandate such as government internal auditors, ministers, judiciary, parliament, and state audit institutions) and informal oversight institutions (i.e. civil society organizations, academia, the media) systematically monitor how the armed, police and security forces make use of public funds

   ii. parliamentary, judiciary and audit authorities detect, investigate and address flaws and violations by security and defence actors of financial accountability laws, regulations, and policies

   iii. administrative-disciplinary or criminal proceedings are enacted against security and defence personnel found guilty of mismanagement or corruption

   iv. sensitive spending such as covert spending and black budgets should be audited in special ways, adapted to the nature of the activities they are meant to finance, but should never be exempt from being monitored

   v. civil society, the media and academia conduct public debates and research to identify the financial flaws in the security system and estimate the costs of the country's past and future human, economic and security needs. This research and these debates are considered part and parcel of the fundamental right to know and free speech

Although in many cases, the proliferation of extrabudgetary funds is due to weaknesses in the budgeting and financial management system of a country, those funds may still be necessary. However, governments should strive to develop sound transparent budgeting and public financial management systems instead of relying on the creation of extrabudgetary funds.

[30] Geneva Center for Security Sector Governance (DCAF), *International Standards of Financial Oversight in the Security Sector* (2015), https://securitysectorintegrity.com/wp-content/uploads/2017/02/International-Standards-of-Financial-Oversight_ENG.pdf.

10. Integrity in Defence Procurement

Prof. Todor Tagarev

Introduction

Russia's large-scale aggression against Ukraine, launched in February 2022, changed fundamentally the security landscape for Europe, NATO, and for many of its partners. In the fourth year of the war, many European leaders admit that Europe needs to be ready to fight a further Russian aggression in five years or, possibly, even sooner. This threat perception was translated into decisions to increase significantly defence expenditure. Several NATO members already spend about 4% of their GDPs on defence. In three years, from 2021 until 2024, the defence expenditure of EU member states grew by 31%, and defence investments doubled, exceeding EUR 100 billion.[1]

At the 2025 Hague Summit, NATO members committed to investing 5% of GDP annually in core defence requirements and defence and security-related spending by 2035. Of this, at least 3.5% of GDP annually will be based on the agreed definition of NATO defence expenditure, while up to 1.5% annually will be dedicated to critical infrastructure protection, network security, civil preparedness and resilience, accelerating innovation, and strengthening the defence industrial base.[2]

In March 2025, the European Commission published a White Paper for European Defence, providing opportunities to spend an additional EUR 800 billion on defence in the next four years and thus approach the 3.5% commitment. Further, the White Paper emphasizes the multinational procurement of defence capabilities and investments in rapidly developing drone and anti-drone systems, as well as emerging and potentially disruptive technologies such as artificial intelligence, quantum, cyber, and electronic warfare technologies.[3]

A significant portion of the increase in expenditures will be allocated to procurement. The NATO target of allocating 20% of national defence budgets to research and development and capital investments is now history. All NATO members are expected to invest more in new technologies, materiel, and networks. The United Kingdom, for example, was spending around 25% of its defence budget on investments. This percentage rose to 35% in 2023–24, and is expected to rise to 43% by 2028–29.[4]

The commitment to this significant increase in defence investments is an important political signal to NATO's opponents, friends, and societies. However, some analysts define the current economic context for raising the defence expenditures as 'sobering,' with relatively high levels of public debt and sluggish economic growth. Others note the expected widening in the gap in investments needed to meet green and social goals, including climate risk mitigation, healthcare, education, and housing.[5]

In this environment, any news on corruption in defence will negatively affect public support for higher defence budgets. Procurement, as one of the defence activities traditionally most susceptible to corruption, will be under increased scrutiny. This chapter, therefore, looks into the corruption risks related to procurement, setting it in the broader discipline of defence acquisition. It outlines the principles and general guidelines in strengthening the integrity of defence procurement. There is, then, a presentation of good practices in building integrity at the

[1] European Commission, *Joint White Paper for European Defence Readiness 2030*, JOIN(2025) 120 final, March 19, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0120.
[2] The Hague Summit Declaration, issued by the NATO Heads of State and Government participating in the meeting of the North Atlantic Council in The Hague 25 June 2025, Press Release 2025 001, June 25, 2025, https://www.nato.int/cps/en/natohq/official_texts_236705.htm.
[3] *Joint White Paper for European Defence Readiness 2030*.
[4] Bee Boileau and Max Warner, "UK defence spending: composition, commitments and challenges," Institute for Fiscal Studies, September 26, 2025, https://ifs.org.uk/publications/uk-defence-spending-composition-commitments-and-challenges.
[5] Sebastian Mang, "European defence spending soars, but climate and care are still 'unaffordable'?" New Economics Foundation, June 23, 2025, https://neweconomics.org/2025/06/european-defence-spending-soars-but-climate-and-care-are-still-unaffordable (accessed February 23, 2026).

process, organizational, and individual levels. The chapter includes examples on the role of civil society organizations and data analytics in strengthening the integrity of defence procurement.

This text builds on and amends the section on integrity in the defence procurement chapter from the 2010 Compendium.[6] An interested reader will find additional, and still valid information in the 2010 version, for example on: integrity pacts; providing channels for reporting suspected cases of corruption and whistleblowers' protection. There are also chapters on the related topics of offsets and the use of surplus equipment and infrastructure.

Corruption Risks and Impact

Defence procurement often involves considerable amounts of money. Procurement requirements and the assessment of potential solutions and delivered products rely on highly specific expertise and often include classified information. Deliveries may extend over several years, while the actual effect of associated offset or industrial cooperation arrangements needs to be monitored and evaluated over decades. Box 10.1 provides further examples of corruption risks related to procurement. These and other factors limit the transparency and increase the marginal cost of corruption and fraud and decrease the marginal benefits. Hence, officials and contractors with low ethical standards are tempted to abuse procurement processes for personal benefit.

The impact of corruption in procurement ranges widely from squandering public resources through lower capability levels, to negative impact on mission objectives and loss of life. For example, the 2021 lessons learned report by the Special Inspector General for Afghanistan Reconstruction (SIGAR) admitted that 'pervasive corruption put U.S. funds sent through the Afghan government at risk of waste, fraud, and abuse.' Apparently, Afghan officials were corrupting reconstruction efforts, which exacerbated the conflict and drove many Afghans towards the Taliban.[7] The ultimate effect was the quick collapse of the Afghan government once the U.S. and coalition forces left the country.

Another example relates to fraud in providing logistics services. A U.S. Air Force F-16 pilot was killed in 2020 in a fatal jet crash, when his ejection seat parachute failed to deploy. The Office of Special Investigations has opened a procurement probe into the possible supply of counterfeit or defective parts by a contractor.[8]

Box 10.1. Main Corruption Risks in Defence Procurement

[Author: Francois Melese]

Defence procurement represents the most significant corruption risk area because of the complex, high-value nature of military contracts. The greatest risks stem from the inherent secrecy, the large sums involved, the technical complexity that can obscure biases, and the close working relationships and 'revolving doors' between defence officials and industry representatives.

Major risks include:

- Inflated or wasteful procurement costs, especially for undeveloped or rapidly procured equipment. Inflated contract values through collusive bidding or specification manipulation can increase costs.
- Substandard gear and logistics due to misappropriated contracts, impacting combat effectiveness. Ongoing support contracts for weapons systems are particularly vulnerable as they

[6] "Defence Procurement," in *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices*, ed. Todor Tagarev (Geneva: NATO & DCAF, 2010), pp. 72-85.
[7] Special Inspector General for Afghanistan Reconstruction, *What We Need to Learn: Lessons from Twenty Years of Afghanistan Reconstruction*, August 2021, https://www.govinfo.gov/content/pkg/GOVPUB-S-PURL-gpo159506/pdf/GOVPUB-S-PURL-gpo159506.pdf.
[8] Rachel S. Cohen, "An F-16 pilot died when his ejection seat failed. Was it counterfeit?" *Air Force Times*, September 14, 2022, https://www.airforcetimes.com/news/your-air-force/2022/09/13/an-f-16-pilot-died-when-his-ejection-seat-failed-was-it-counterfeit/ (accessed February 23, 2026).

often lack competitive oversight and involve long-term relationships between individual contractors and defence officials.

- Misallocation during emergency rearmament, particularly when oversight is reduced.

Further NATO and partner nations often face the dual challenge of whether to become more involved in defence business ('make'), or turn more business over to the private sector ('buy'). Make-or-buy decisions include both traditional short-term defence contracts, as well as longer-term public-private partnerships (PPPs). Today partnering is used to support a broad spectrum of military activities: from logistics, cyber security, humanitarian assistance and disaster relief, to the provision of military housing and theatre sustainability.[9]

Well-structured contractual agreements allow both public and private-sector participants to leverage and maximize the use of their joint resources to accomplish military objectives more efficiently and effectively. Still, while there is great potential from partnering, there are also risks.

General Principles and Guidelines for Integrity in Procurement

Procurement is an activity with high corruption risks, but in the public sphere generally. Article 9 of the United Nations Convention Against Corruption (UNCAC, 2004) outlines some main principles of preventing corruption in public procurement, with a focus on increasing transparency, competitiveness, and objective decision-making. It further calls for public distribution of information on tenders, selection criteria, contracts, procedures for appealing decisions, and for setting in place a system of screening, training, and declaration of potential conflict of interests of personnel responsible for procurement.[10]

The 2004 public procurement directive of the European Union, replaced in 2014 by Directive 2014/24/EU, and in particular the Organisation for Economic Co-operation and Development (OECD) in its principles for integrity in public procurement, further detail the UNCAC guidelines. Box 10.2 below summarizes the OECD principles.

While implementation may require taking some specific circumstances into account, these principles are valid for the procurement of products and services by military and defence organizations. Box 10.3 elaborates on the principles of the EU general public procurement directive and their translation into Directive 2009/81/EC regulating procurement in the fields of defence and security.

[9] For example, the U.S. military employed one contractor for every seven soldiers for its theatre sustainability during World War II; the ratio was one-to-one in Iraq, and at its peak in the Afghan theater, the U.S. employed three contractors for every one soldier. See, for example, Mark Cancian, "In Afghanistan, Contractors Were Unsung Heroes of US Efforts," *Breaking Defence*, August 30, 2021, https://breakingdefense.com/2021/08/in-afghanistan-contractors-were-unsung-heroes-of-us-efforts/ (accessed February 23, 2026).
[10] United Nations Office on Drugs and Crimes (UNODC), United Nations Convention Against Corruption (Vienna: UNODC, 2004), https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.

Box 10.2. Integrity Principles of the Organisation for Economic Co-operation and Development

[Author: Anela Duman]

OECD integrity principles are a set of guidelines that promote good governance, anti-corruption, and transparency in both the public and private sectors. Their proper implementation will reduce corruption risks in public procurement. They will also provide policy makers with a vision for public integrity long-term strategy that has a risk-based, context dependent, behavioural approach for developing an integrity culture.

The OECD identifies a number of interconnecting principles which may, directly or indirectly, prevent corruption and improve good governance and accountability in public, and defence and security procurement. These principles include:[11]

- Providing an adequate degree of transparency in the entire procurement cycle with the aim to promote fair and equitable treatment for all potential suppliers;
- Maximizing transparency in competitive tenders and taking measures to enhance integrity, particularly as relates to exceptions to competitive tendering;
- Ensuring that public funds are used in public procurement according to intended purposes;
- Ensuring that procurement officials have adequate professional knowledge and skills and meet the highest integrity standards;
- Setting in place mechanisms to prevent risks to integrity in public procurement;
- Encouraging close cooperation between public and private sectors to meet high standards of integrity in contract management;
- Providing specific mechanisms for monitoring public procurement, detecting misconduct, and applying sanctions accordingly;
- Establishing a clear chain of responsibility and effective control mechanisms;
- Handling complaints from potential bidders and suppliers in a fair and timely manner;
- Empowering civil society organizations, media and the wider public to scrutinize public procurement.

The OECD provides also practical guidelines for implementing these principles and enhancing integrity at each stage of the procurement cycle.[12]

[11] Organisation for Economic Co-operation and Development*, OECD Principles for Integrity in Public Procurement* (Paris: OECD, 2009), https://www.oecd.org/en/publications/2009/03/oecd-principles-for-integrity-in-public-procurement_g1gh9fbe.html.
[12] Ibid., pp. 51-73.

Box 10.3. Impact of EU Procurement Directives on Integrity

[author: Anela Duman]

The general procurement regulations in the European Union aim to strengthen the single internal market, prohibiting discrimination between member states and encouraging increased transparency. Directive 2004/18/EC made it obligatory for member states to exclude suppliers who have been found guilty of corruption or of fraud, or who otherwise participated in a criminal organization, from public tenders.[13] It was later replaced by new Directive 2014/24/EC. It further emphasized that each procurement procedure needs to be duly documented to allow traceability and transparency in decision-making. These are seen as essential factors for ensuring sound procedures and for efficient measures against corruption and fraud.

Directive 2004/18/EC allowed exceptions for defence procurement cases when they are related to essential national security interests. In such cases, member states must prove the necessity of the exemption.

In 2009, the European Parliament and the Council approved Directive 2009/81/EC regulating procurement in the defence and security fields. It reaffirmed the principle of transparency and the exclusion of economic operators who have been found guilty of corruption, fraud, or money laundering, adding the financing of terrorism and other terrorism-related offences. It also regulated defence specific issues, such as the protection of classified information, supply chain security, and sub-contracting. The Directive stipulates few carefully defined specific exclusions, such as contracts awarded pursuant to international rules and contracts supporting forces deployed outside European Union territory when operational needs require the involvement of suppliers located in the operation area.

The following sections examine the implementation challenges and present good practices in assuring the integrity of decision-making processes, organizations, and personnel involved in defence procurement.

Integrity of the Defence Procurement Process

Building new defence capabilities often requires years, or even decades when current technologies do not meet capability requirements. Thus, defence procurement is part of the much broader field of *defence acquisition* that involves activities for identifying the requirements to meet the needs of the user, procuring them, ensuring support throughout their useful lifecycle and providing for their eventual disposal. Figure 10.1 illustrates the process of defence acquisition. The process is usually initiated by the prospective user, in most cases, a command authority, by identifying and documenting an operational need. It may be based on a change in policy or threat landscape, technological advancement, a change in doctrine, or lessons learned from past or ongoing operations.

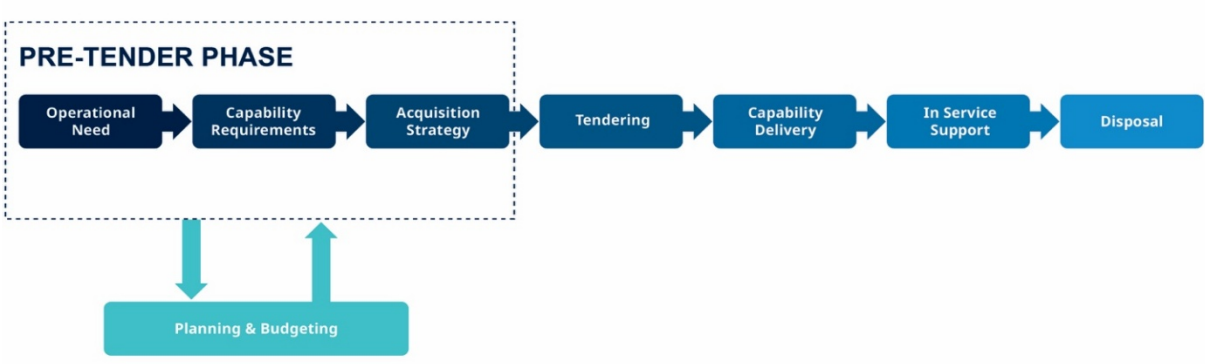


Figure 10.1: Defence Acquisition Process.

[13] Sope Williams, "The Mandatory Contractor Exclusions for Serious Criminal Offences in UK Public Procurement," *European Public Law* 15, no. 3 (2009): 429-444, https://doi.org/10.54648/euro2009031.

Defining capability requirements is, in itself, a complex process, starting with identification of high-level goals and objectives, and desired outcomes. Then requirements are defined in terms of tasks to be performed in specified conditions, or scenarios, and standards to be followed. The definition includes measures of effectiveness. It is important to note that, at this stage, requirements are not tied to a particular technological or organizational solution.

The elaboration of an acquisition strategy for an approved operational need and the respective capability requirements aims to design and evaluate acquisition options and to select the best option. The options may span several key dimensions, such as:

- develop a new solution ('make') or select from commercial- or military-off-the shelf products (for the make-or-buy dilemma see also Box 10.1);
- buy nationally (just for the own armed forces) or create/join a multinational development and procurement initiative;
- competition, e.g. organize international or national competitive bidding, limited competition, sole sourcing;
- technological level, e.g. from meeting basic interoperability requirements to providing superiority over any potential opponent;
- maintenance, e.g. organic (within the armed forces), cooperation with the armed force of allies and partners, third party maintenance, and maintenance by the original equipment manufacturer.[14]

In addition, the acquisition strategy will consider political, economic, and security options, such as bilateral and allied relations (e.g. joining the European Union's capability coalitions), industrial cooperation and technology transfer, security of operation and supplies, etc.

Strategy options may have very different levels of performance and great variations in cost. Timescales may also vary considerably, especially when equipment and/or services are not purchased off-the-shelf. A good practice is to discuss trade-offs with key stakeholders and document all main considerations in selecting an option.

For the selected option, the required defence capability is described by integrating the DOTMLPFI components (i.e. Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Interoperability) to ensure that capability can effectively achieve desired effects. The DOTMLPFI representation of a capability will guarantee that all materiel needs, i.e. equipment, infrastructure, and maintenance capacity will be accounted for in procurement, and the capability options can be properly costed.

The option chosen will be informed in the process of interaction between defence planning and budgeting and the definition of capability requirements and an acquisition strategy (as illustrated in Figure 10.1). A mismatch between the full cost of the selected option and the resources allocated in mid- and longer-term will have a detrimental impact on the transparency of the acquisition process and, most likely, on the capability level achieved.

Given the large amounts of resources associated with and the long-term effect for acquisition decisions, a good practice is to conduct dedicated Operations Research/ Operational Analysis studies to define (or refine) and compare acquisition options using mathematical and analytical models and rigorous modelling. The System Analysis and Studies panel of NATO's Science and Technology Organization is a platform for such studies, many of which are open to partner countries.[15] Also, many allied countries have MoD integral Operational Analysis units or work with academic departments, both positioned outside the chain of command and providing unbiased professional advice on options. At later stages of the acquisition process the same units may be tasked with assessing to what extent procurement projects have delivered.

[14] This elaboration builds on Elisabeth Wright, "Twenty First Century Defense Acquisition: Challenges and Opportunities," *Connections: The Quarterly Journal* 5, no. 1 (2006): 71-80, https://doi.org/10.11610/Connections.05.1.06.
[15] For published studies of the System Analysis and Studies panel see https://www.sto.nato.int/publications/.

Another good practice in view of involving parliaments, industrial and societal stakeholders is to present publicly at least a partial unclassified version of an overall defence investments plan and seek parliamentary approval of it. Preliminary approval might also be required for projects valued above a certain threshold. This approach provides a high degree of transparency and opportunities to hold the executive to account for outcomes and performance. It also helps to reveal discrepancies and potential cases of corruption or mismanagement, and thus maintains societal support for increased defence expenditures.

Achieving process integrity means ensuring that every stage of decision-making–from identifying an operational need, defining capability requirements, choosing an acquisition strategy, making procurement decisions, contracting and managing contracts, through to in-service support, utilization, and decisions about involving national defence or dual-use industry–is transparent and traceable. It also requires that each stage can be audited, especially in terms of outcomes, policy alignment, and value for money. Furthermore, decisions need to be based on verifiable data and evidence. Finally, the traceability needs to be preserved in a changing threat, technological and fiscal environment.

A particular challenge is the slow adaptation, or sometimes a lack of adaptation, to such changes in acquisition decisions. This may be a sign of poor integrity. For example, the U.S. Army cancelled the Future Attack Reconnaissance Aircraft (FARA) programme in 2024 after investing USD 2.4 billion in it due to the growing role of reconnaissance and attack drones in modern warfare. This is an example of how expensive military programs may become obsolete before deployment. The question is: 'why was such an outdated concept pursued for years? The answer lies in the procurement cycle itself, this is secure long-term funding, when obsolescence becomes undeniable, programmes are quietly abandoned without financial repercussions for those involved.'[16] This is one of the examples demonstrating that acquisition decisions, even if partially implemented, need to be regularly reviewed and confirmed or adapted. And this needs to be done while preserving the traceability and supporting evidence.

Overall, there are numerous examples of good practice building integrity and reducing corruption risks in standardized procurement processes that may take years or even decades. Much less experience is available in cases of short innovation cycles, such as in drone, anti-drone, and electronic warfare solutions in the ongoing war of Russia against Ukraine. There fighters can rely on a certain technological advantage for several months, or even weeks, and need new solutions to maintain their edge. NATO approaches this challenge by aiming to increase the agility of defence organizations and speed up innovation. As part of this approach, NATO's Allied Command Transformation (ACT) leads the NATO Innovation Challenge. It tasks start-ups, universities, and industry, working jointly with the military, to deliver creative solutions that are tested, refined, and made available to war fighters in months. In early 2025, the Challenge focused on affordable, layered defences against Russian glide bombs and Shahed-type drones. Within 70 days, three solutions 'moved from concept to live-fire demonstration: AI-enabled software predicting impact zones in seconds, a reusable interceptor drone combining jamming with kinetic effect, and an expendable swarm creating a denial bubble.'[17] These three solutions were scheduled for live intercept trials by Ukrainian air defence units and operational deployment before the end of 2025.

[16] B. Arneson, Jack Cinamon, Alexandra Fischer et al., *Tracing Corruption: Emerging Patterns in the Global Arms Trade* (World Peace Foundation, August 2025), p. 15, https://worldpeacefoundation.org/publication/tracing-corruption-emerging-patterns-in-the-global-arms-trade/.
[17] NATO ACT, "Driving Agility in Allied Defence: The Role of the NATO Innovation Challenge," *Horizons*, September 2, 2025, https://www.linkedin.com/pulse/driving-agility-allied-defence-role-nato-innovation-challenge-ko8fe/.

Box 10.4. Speeding Up Drone Delivery

In the fourth year of the ongoing Russo-Ukraine war, the Ukrainian Armed Forces expect to receive over two million drones of dozens of different types.[18] Increasingly relying on drone warfare, Russia and Ukraine play a cat-and-mouse game, with fast innovation cycles for drones and counter-drone technologies.[19] New technological developments provide an advantage for only months, or even weeks, before the other side adapts. Heavily centralized procurement systems adhering to a traditional acquisition cycle from establishing a mission need and defining requirements to deployment are clearly inadequate. The Ukrainian defence ministry, therefore, implements two new approaches to speed up procurement (in addition to volunteer donations allowing units to buy drones directly from suppliers).

First, in December 2024 the Ukrainian ministry piloted, and then expanded its 'Drone Line' programme and allocated EUR 57 million per month to the five units most successful in using uncrewed aerial vehicles (UAVs) to buy drones, electronic warfare equipment, and vehicles for mobile UAV groups.[20] This initiative is expected to create a more flexible military system, allowing for the rapid fulfilment of diverse frontline requirements. It helps diversify the types of weapons available to units, moving beyond a single source of supply. Finally, by allowing frontline units to acquire specialized equipment, the initiative supports the rapid development and adoption of new drone technologies to counter evolving threats from Russia.

In the summer of 2025, Ukraine launched a second initiative called 'DOT-Chain Defence Marketplace.' It allows frontline units to place orders for FPV drones through an IT system, developed by the State Operator for Non-Lethal Acquisition (DOT) and operated by the ministry's Defence Procurement Agency (DPA). In the first two weeks of the piloting phase, DPA delivered 7,000 drones for approximately EUR 5 million in two weeks – four times faster than the standard procedure. In addition, joint DOT-DPA teams conduct special training for units, including on-site visits to the combat zone. Upon the successful completion of the piloting phase, DOT-Chain Defence will be scaled up to allow the participation of more military units. The list of available equipment for ordering will be expanded to include electronic warfare and signals intelligence, electronic intelligence systems, ground robotic systems, more types of UAVs, and related munitions.[21]

Organizational Integrity

Organizational integrity goes beyond compliance with legal norms; it is the alignment of decisions and actions with the organization's values and ethical principles. Enhancing organizational integrity requires ethical leadership, communication, accountability of all members, and continuous improvement. In relation to defence procurement, organizational integrity requires setting rules, regulations, and policies to prevent the penetration of commercial interests and to guarantee professional independence. Setting a policy for lobbying, rules and procedures for exchange of procurement-related information between defence ministries and economic actors, and a 'revolving door' policy enhance [22] organizational integrity.

Regarding independence, Chapter 4 of this volume provides examples of establishing defence acquisition agencies[23] in NATO countries as separate legal entities. While working to meet the requirements set most often

[18] Ministry of Defence of Ukraine, "Ministry of Defence has supplied 1 million FPV drones to the Armed Forces of Ukraine since the start of the year," August 1, 2025, https://mod.gov.ua/en/news/ministry-of-defence-has-supplied-1-million-fpv-drones-to-the-armed-forces-of-ukraine-since-the-start-of-the-year.
[19] Ulrike Franke, "Drones in Ukraine: Four lessons for the West," Commentary, European Council on Foreign Relations, January 10, 2025, https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/.
[20] Vadim Kushnikov, "Combat Brigades of Armed Forces Received Over UAH 12 Billion for Drones and Special Equipment," *Militarnyi*, March 28, 2025, https://militarnyi.com/en/news/combat-brigades-of-armed-forces-received-over-uah-12-billion-for-drones-and-special-equipment/.
[21] Ministry of Defence of Ukraine, "The Ukrainian military received the first thousand drones through the DOT-Chain Defence weapons marketplace," August 13, 2025, https://mod.gov.ua/en/news/the-ukrainian-military-received-the-first-thousand-drones-through-the-dot-chain-defence-weapons-marketplace.
[22] Transparency International defines 'revolving door' as "the movement of individuals between positions of public office and jobs in the same sector in the private … sector, in either direction." It can be abused in private interests. Some NATO members impose by law a "cooling off period" – the minimum time required between switching from the public to the private sector. See https://www.transparency.org/en/corruptionary/revolving-door.
[23] May also be called procurement or materiel agencies or organizations.

by military commands, they apply professional acquisition management principles and methods, including a quest for efficiency, e.g. value for money. A similar arrangement was adopted by Ukraine's defence ministry in its war with Russia. Box 10.5 provides details.

Most procurement organizations have their internal 'integrity watchdogs,' while their activities are subject to monitoring and investigation by bodies outside the defence sector. For example, the U.S. Justice Department created the Procurement Collusion Strike Force (PCSF) in 2019 in a joint law enforcement effort to combat antitrust crimes and related fraudulent schemes that affect government procurement at all levels of government. PCSF was instrumental, for instance, in revealing fraud and bringing to court a contractor and a federal governmental official for their roles in schemes to rig bids, paying and receiving bribes in connection with the sale of IT products and services to the U.S. federal government purchasers, including the Department of Defense.[24] The organization needs to adapt continuously to preserve its integrity. Cooperation with civil society organizations may sustain the drive for integrity in procurement, even in wartime, and increase societal trust in the military. Box 10.6 highlights the role of StateWatch in the continuous reform of Ukraine's defence procurement system by strengthening transparency and building integrity.

Two other and interrelated issues are relatively new and have not been the subject of rigorous exploration: tasking international/ multinational organizations with procuring equipment or services for national armed forces and multinational procurement. As stated in the White Paper for European Defence and follow-on documents, a considerable portion of the increase in the defence expenditures will be dedicated to multinational procurement using *ad-hoc* arrangements or existing multinational agencies, such as the European Defence Agency or the Organisation for Joint Armament Co-operation (OCCAR – Organisation Conjointe de Coopération en matière d'Armement).

Box 10.5. Reforming Ukraine's Defence Procurement System

[Author: Vlasta Kovbasa]

In 2022, amid a large-scale war and with support from civil society and international partners, Ukraine launched a reform of its defence procurement system – an essential step toward strengthening integrity in the defence and security sector. The country adopted a two-tier system: the Ministry of Defence set procurement policies, while two new legal entities'–the Defence Procurement Agency (DPA) and the State Operator for Non-Lethal Acquisition (DOT)–handled implementation. The DPA established an internal oversight system, requiring commercial offers to be simultaneously reviewed by multiple departments and deputy directors.[25] This approach aimed to prevent intermediary-driven corruption schemes by ensuring that proposals from companies could not be ignored by single officials or intercepted by intermediaries, supporting the 'all see all' principle.

Bill No. 8381, developed with the expert support of the Anti-Corruption Action Centre (AntAC), was adopted in 2023. It provided for the publication of prices for goods and services purchased for army's needs (excluding weapons) in the Prozorro[26] public procurement system.[27] As a result of this legislative reform and increased transparency, DPA was able to purchase 2,000 DJI Mavic drones at an average price of UAH 173,000 each

[24] U.S. Department of Justice, "Four Defendants Plead Guilty in Ongoing Bid-Rigging, Fraud and Bribery Investigation Related to U.S. Government IT Purchases," Press Release, Archives, January 14, 2025, https://www.justice.gov/archives/opa/pr/four-defendants-plead-guilty-ongoing-bid-rigging-fraud-and-bribery-investigation-related-us.

[25] Anti-Corruption Action Center (AntAC), *"Arsen Zhumadilov Dismissed Artem Sytnyk from the Position of Deputy Director of the Defense Procurement Agency, Undermining the System That Allows Buying Weapons Without Intermediaries,"* April 17, 2025, https://antac.org.ua/news/arsen-zhumadilov-zvilnyv-artema-sytnyka-z-posady-zastupnyka-dyrektora-aoz-tse-mozhe-zruynuvaty-systemu-iaka-dozvoliaie-kupuvaty-zbroiu-bez-prokladok.

[26] The Prozorro electronic public procurement system is an online platform where state and municipal contracting authorities announce tenders for the procurement of goods, works, and services, and businesses compete in bidding to win the opportunity to supply them to the state. See here: https://prozorro.gov.ua/en.

[27] Anti-Corruption Action Center (AntAC), *"No more no eggs for 17 and potatoes for 22? The Rada adopted a bill that will force the Ministry of Defence to publish procurement prices per unit for the Armed Forces"*, February 24, 2023, https://antac.org.ua/news/bilshe-bez-iaiets-po-17-i-kartopli-po-22-rada-pryyniala-zakonoproiekt-iakyy-zmusyt-minoborony-pokazaty-tsinu-zakupivel-dlia-zsu-za-odynytsiu-produktsii/.

(approximately EUR 3,500) and secured a 15% price reduction on winter boots in a contract valued at nearly UAH 900 million (approximately EUR 18 million), in both cases providing highly cost-effective outcomes.[28]

In October 2024, the Minister of Defence appointed a Supervisory Board for the Defence Procurement Agency to ensure transparent and fair arms procurement. The Supervisory Board included international experts from France and Poland, as well as respected civil society figures.[29] The establishment of the Agencies' Supervisory Boards aligned with one of the recommendations in NATO's Strategic Defence Procurement Review.[30]

Notably, in January 2026, the State Operator for Non-Lethal Acquisition (DOT) was integrated into the Defence Procurement Agency. While some considered this move as risky, others praised it for reducing costs, improving efficiency, and enhancing transparency in management.[31]

Box 10.6. The Role of CSOs in Strengthening Transparency in Defence Procurement

[Author: Vlasta Kovbasa]

As one of Ukraine's leading NGOs, StateWatch illustrates the role of civil society in strengthening transparency and accountability in Ukraine's defence procurement system by monitoring defence spending and delivering analytical support to government bodies.[32] In particular, it has supported the Ministry of Defence in developing the *PartnerMOD* portal, a platform that connects the Ministry with manufacturers of non-lethal goods.[33] This digital solution streamlines compliance certification and expands the supplier base, thus lowering the risk of abuse by individual officials and ensuring greater transparency across the procurement process.[34] Furthermore, StateWatch provided technical support for DOT Chain – an innovative system that manages the logistics requirements of Ukraine's Armed Forces by consolidating documentation within a single platform and automating key processes, resulting in a fourfold reduction in delivery times.[35]

StateWatch also continuously monitors the implementation of the NATO-Ukraine Strategic Defence Procurement Review, which aims to align Ukraine's defence procurement with Euro-Atlantic practices.[36] In its 2025 analytical reviews, StateWatch highlighted steps taken by the Defence Procurement Agency (DPA) and the State Operator for Non-Lethal Acquisition (DOT) to improve their internal compliance systems, including DOT's 'blacklist' of suppliers that fail to fulfil their obligations and DPA's verified suppliers registry.[37] The reviews also noted progress in digitalizing procurement by scaling up the DOT-Chain Defence, launching the Defence City legal regime, and expanding cooperation with NATO agencies.[38] Additionally, both DPA and DOT received ISO 37001 certification, demonstrating conformity with international standards.[39]

[28] Anti-Corruption Action Center (AntAC), *"Results of May,"* June 10, 2024, https://antac.org.ua/news/zvit-tspk-za-traven/.
[29] Anti-Corruption Action Center (AntAC), *"Results of October,"* November 12, 2024, https://antac.org.ua/news/zabraly-u-koruptsioneriv-mozhlyvist-vidkupliatysia-vid-pokarannia-zvit-tspk-za-zhovten/. See also AntAC's Facebook post from October 14,2024, https://www.facebook.com/story.php?story_fbid=946875710577117&id=100057640893390&mibextid=WC7FNe&rdid=BMLhHZc4r00DtQ8H#.https://antac.org.ua/news/zabraly-u-koruptsioneriv-mozhlyvist-vidkupliatysia-vid-pokarannia-zvit-tspk-za-zhovten/.
[30] Daria Kalenyuk, "Urgently Appoint Supervisory Boards in the DPA and DOT – NATO's Recommendation for Ukraine," *Ukrainska Pravda*, August 19, 2024, https://blogs.pravda.com.ua/authors/kalenuik/66c3066e7a355/#google_vignette.
[31] StateWatch, *The State Logistics Operator's Final Month: A StateWatch Monitoring Report, December 2025*, February 25, 2026, https://statewatch.org.ua/en/publications/strong-the-state-logistics-operator-s-final-month-a-statewatch-monitoring-report-december-2025-strong/; Volodymyr Tunik-Fryz, "DPA and DOT to be merged by January 2026: the Ministry of Defence's Public Council has criticised the move," *Economichna Pravda*, October 6, 2025, https://epravda.com.ua/oborona/aoz-i-dot-ob-yednayut-do-2026-roku-812488/.
[32] StateWatch, *StateWatch Annual Report 2024,* July 16, 2025, https://statewatch.org.ua/en/reports/statewatch-annual-report-2024/.
[33] See Ministry of Defence of Ukraine, *Partner MOD*, https://partner.mod.gov.ua (accessed February 23, 2026); StateWatch, *StateWatch Annual Report 2024,* July 16, 2025, https://statewatch.org.ua/en/reports/statewatch-annual-report-2024/.
[34] StateWatch, *StateWatch Annual Report 2024.*
[35] Ibid.; Ministry of Defence of Ukraine, "How to use the new DOT-Chain system and what are its benefits," October 9, 2024, https://mod.gov.ua/explanation/yak-koristuvatisya-novoyu-sistemoyu-dot-chain-ta-v-chomu-yiyi-korist.
[36] StateWatch, *NATO-Ukraine Strategic Defence Procurement Review StateWatch Implementation Monitoring April-June 2025,* July 9, 2025, https://statewatch.org.ua/en/publications/nato-ukraine-strategic-defence-procurement-review-statewatch-implementation-monitoring-april-june-2025/.
[37] Ibid.
[38] StateWatch, *NATO-Ukraine Strategic Defence Procurement Review StateWatch Implementation Monitoring June-November 2025*, January 8, 2026, https://statewatch.org.ua/en/publications/nato-ukraine-strategic-defence-procurement-review-statewatch-implementation-monitoring-june-november-2025/.
[39] Ibid.

Good building integrity practices in national defence procurement are also applicable, and applied, to multinational procurement initiatives and the implementing agencies. One example is OCCAR with a core-business of managing of complex, cooperative defence equipment programmes through their life cycle. Belgium, France, Germany, Italy, Spain and the United Kingdom are OCCAR member states, and nine other NATO countries are non-member participating states.[40] OCCAR manages some of the biggest European equipment projects, such as the multi role armoured vehicle Boxer, the A400M transport aircraft, and the Horizon MLU/FREMM multi mission frigates.

OCCAR does not have a specific "anti-corruption" programme, but integrity measures are embedded in its operational framework. These include a strong emphasis on security, internal controls, and ethical conduct. Measures involve a comprehensive business management system, certified according to ISO 9001:2015; internal control processes for operational effectiveness and compliance; a security agreement that outlines procedures for handling breaches and information security; ethical leadership; and management of conflicts of interest in its public-private interactions.[41] If deemed necessary, the Board of Supervisors may order an inspection or audit of OCCAR.[42] The organization's goal is to ensure that armaments cooperation is managed in a way that is efficient, effective, transparent, accountable, and compliant with laws and regulations.

Integrity of Personnel Involved in the Acquisition, Sustainment and Utilization of Materiel

Ensuring integrity in defence procurement involves creating and implementing clear policies, including codes of ethics, robust oversight, and regular training to prevent, identify, and report cases of conflict of interest and corruption. Training may include case studies on manipulation at any stage in the decision chain from defining capability requirements to selling surplus weapon systems and materiel.

As a rule, defence procurement requires highly technical expertise and operational and tactical knowledge. Therefore, one issue, specific to defence, is the risk of corruption related to officials moving directly from a position of authority in the military organization to employment with a supplier. A good practice is to legally restrict such 'revolving door' practice (briefly examined above) and to enforce implementation.

Notwithstanding, the sensitivity of the information on military and civilian defence personnel, many NATO countries have introduced legal norms and procedures, applicable to everyone with a role in procuring material or services. These norms increase the transparency of the financial and material status of all such individuals. In many cases, they require, for instance, the annual declaration of income, financial deposits, loans, investments, and acquisition of high-value assets, including real estate, of the official, their spouse/cohabitant, and minor children. These declarations are public and need to be provided for a period after the individual has left the defence organization.

Such data, along with data from other sources, can be used to reveal cases of potential corruption or other types of conflict of interest.

Data Analytics and AI in support of Procurement Integrity

Data analytics can help detect defence procurement fraud and corruption. Based on data from tender procedures, suppliers, and pricing, network analysis may reveal bidding patterns, price clustering, and supplier overlaps, indicative of bid rigging and collusion. Entity resolution and the analysis links between addresses, directories, and bank accounts from vendor registries, tax records, and personnel databases can reveal conflict of interest and insider deals. Anomaly detection and predictive cost models on the basis of contract and payment

[40] OCCAR, "About us," https://www.occar.int/about-us.
[41] Organisation for Joint Armament Co-operation (OCCAR), "OCCAR Case Study," *Auditing procurement of major armament projects workshop of the European Court of Auditors*, May 2019, https://www.eca.europa.eu/sites/eca-audit-defence/EN/Documents/Guillaume%20Bigot%20-%20Auditing%20procurement%20of%20major%20armament%20projects.pdf.
[42] OCCAR, Convention on the Establishment of the Organisation for Joint Armament Cooperation.

data may indicate overpricing and false invoicing. Cross-matching business registries and financial disclosures may facilitate the identification of fake invoices and shell companies.

Several NATO countries already use data analytics tools for such purposes. For example, the U.S. Department of Defense has established a Fraud Reduction Task Force under the 2016 Fraud Reduction and Data Analytics Act. The Defense Contract Audit Agency (DCAA) under the DoD Comptroller and the Defense Criminal Investigative Service (DCIS) under the Inspector General integrate data mining tools into contract oversight.[43] Combining information on contracting officer assignments, vendor award frequencies, and pricing outliers allows for the identification of potential collusion or favouritism.

However, academic research warns that expectations from the application of AI and other data analytics tools in anti-corruption initiatives related to procurement need to be moderated. So far, such tools can provide improvements but not the transformation of anti-corruption oversight and enforcement. The major limitations are due to existing and accessible procurement data and potentially biased datasets and algorithms,[44] as well as flaws in AI technology today such as the risk of hallucinations and sycophancy.

A 2024 report by the U.S. Government Accountability Office also found that data on alleged and settled procurement fraud cases were not always complete and could not always be readily analysed. The same report recommended that data analytics be established as a method for preventing, detecting, and responding to fraud in the respective organizational strategy. It also advised that data be better structured, complete, accessible, and readily subject to analysis and aggregation.[45] Additional measures need to be in place to assure that oversight bodies have access to and are able to integrate information from other relevant repositories.[46]

Conclusion

This chapter attempted to examine the integrity issues in defence procurement comprehensively. It presented internationally recognized principles and examples of good practice in building up the integrity of processes, organizations, and personnel involved in defence acquisition. This treatment is certainly not exhaustive. A number of current and emerging issues require further study, including:

- the enhancement of the transparency and integrity of procurement in meeting urgent operational requirements;
- the procurement of equipment, the maintenance of stockpiles and the upgrading of equipment such as drones, in response to the rapid pace of technological and operational innovation;
- the tension between decision by committee, involving multiple stakeholders and increasing transparency, *versus* the individual responsibility and accountability of senior decision-makers;
- integrity in multinational procurement;
- transparency and integrity in investing public resources in defence industries.

The exchange of information and good practices among participants in the NATO Building Integrity programme can further the understanding and facilitate the national and international efforts in reducing corruption risks in defence procurement.

[43] U.S. Government Accountability Office, *DOD Fraud Risk Management: Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks*, GAO-21-309, (Washington, DC: GAO, 2021), https://www.gao.gov/products/gao-21-309.
[44] Albert Sanchez-Graells, "Procurement Corruption and Artificial Intelligence," in *Routledge Handbook of Public Procurement Corruption*, edited by Sope Williams and Jessica Tillipman (London: Routledge, 2024), https://doi.org/10.4324/9781003220374.
[45] U.S. Government Accountability Office, *DOD Fraud Risk Management: Enhanced Data Analytics Can Help Manage Fraud Risks*, GAO-24-105358 (Washington, DC: GAO, 2024), https://www.gao.gov/products/gao-24-105358.
[46] Chapter 4 of this Compendium also addressed the use of AI in defence procurement.

11. Benefits and Risks of Military Public-Private Partnerships (PPPs)

Francois Melese[1]

'[A public-private partnership] is a cooperative arrangement between [a defence activity] and one or more private sector entities to perform defence-related work…'[2]

Introduction

The global pandemic devastated lives and disrupted economic activity worldwide, forcing governments to assume unprecedented levels of deficits and public debt. While fiscal pressures remain significant, the strategic security environment has shifted dramatically since Russia's full-scale invasion of Ukraine in 2022. NATO Allies committed at the 2025 NATO Summit to allocate up to 5 % of GDP to defence and security-related spending. Despite this increased commitment, ensuring the efficient use of defence resources remains essential. To preserve Alliance capabilities with tight budgets, NATO's smart defence concept encourages collaboration between nations, and between nations and industry. Closer collaboration between defence establishments, industry, and academia, is essential for speeding up innovation and for maintaining a technological and industrial edge, especially in new fields such as artificial intelligence (AI), robotics and hypersonics.[3]

The dual challenge for NATO and partner nations is whether to become more involved in defence business ('make'), or turn more business over to the private sector ('buy'). Make-or-buy decisions include both traditional short-term defence contracts, as well as longer-term public-private partnerships (PPPs). Today, partnering is used to support a broad spectrum of military activities: from logistics, cyber security, military AI applications, humanitarian assistance and disaster relief to the provision of military housing and theatre sustainability.[4]

Ideally, PPPs operate as 'a cooperative venture between the public and private sectors, built on the expertise of each partner that best meets clearly defined public needs through the appropriate allocation of resources, risks, and rewards…'[5] A well-structured PPP allows both public and private-sector participants to leverage and maximize the use of their joint resources to accomplish military objectives more efficiently and effectively. Still, while there is great potential from partnering, it does entail risks.

Military objectives in entering a PPP typically include anything from increasing readiness by adopting new emerging technologies and improving weapon systems and support activities, to leveraging private sector capital and cutting costs. Potential partners can offer valuable proprietary information, unique technical expertise, economies of scale, and learning curve opportunities. The challenge for nations is to find the right private sector partners, and to negotiate, manage, and monitor long-term contracts that provide proper incentives for all parties to satisfy future performance, cost, and schedule requirements.

Traditional defence contracts tend to be short-term, one-sided arrangements. Typically, governments carefully specify performance, schedules, and costs. PPPs, on the other hand, typically involve longer-term collaborative relationships with industry partners. Yet many of the core principles that apply to 'traditional' public procurement also apply to PPPs. According to the UN Commission of International Trade Law (UNCITRAL), a well-

[1] Prof. Melese is Emeritus Professor of Economics, Naval Postgraduate School. Disclaimer: The views expressed belong to the author and do not necessarily represent those of the Naval Postgraduate School, U.S. Navy or Department of Defense.
[2] *Public-Private Partnership for Product Support Guidebook*, Office of U.S. Assistant Secretary of Defense, 2016, p. 3.
[3] Todor Tagarev, Raphael Perl, and Valeri Ratchev, "Recommendations and Courses of Action: How to Secure the Post-Covid Future," in *Transatlantic Security: Securing the Post Covid Future*, edited by IBM (Wien: Federal Ministry of Defence, 2020), pp. 18-41.
[4] For example, the U.S. military employed one contractor for every seven soldiers for its theatre sustainability during the Second World War; the ratio was one-to-one in Iraq, and at its peak in the Afghan theatre, the U.S. employed three contractors for every soldier.
[5] J. Gansler & R. Lipitz, *Moving Toward Market-Based Government: The Changing Role of Government as the Provider*, New Ways to Manage Series (Arlington, VA: IBM Endowment for the Business of Government, 2003).

designed procurement process:[6] a) maximizes economy and efficiency; b) fosters and encourages participation in the process; c) promotes competition; d) provides fair, equal, and equitable treatment of those involved; e) promotes integrity, fairness, and confidence in the process by stakeholders; and (f) achieves transparency in the process.[7]

Box 11.1: Dutch Case Study

[Adapted from *'Managing Integrity in Public-Private Partnerships in the Defence Sector: The Dutch experience developing an adaptive armed forces'* by Dieneke T. de Vos]

Dutch defence forces first took steps to implement their 'adaptive armed forces' concept in 2017 (in Dutch: *de adaptieve krijgsmacht*). This envisions increased collaboration with industry partners to respond better and faster to existing and future threats. The concept aims to improve adaptability, speed, and combat power by embracing rapid technological change and new product and process innovations through systematic exchanges of personnel and materiel with the private sector.[8] According to Dutch Defence Vision 2035, the ultimate objective is to build a smart, technologically advanced defence organization. This organization would be proactive, flexible, rapidly deployable, and self-supporting, with sufficient scalability to adapt to rapidly changing situations. A key challenge is to recognize and mitigate potential integrity-related risks that could arise from closer coordination and collaborative partnerships with the private sector. Anticipated economic, financial, strategic, and operational benefits from partnering reflect the observation that competitive companies must rapidly respond to process and product innovations in the marketplace to ensure the best possible combination of prices/costs and performance. Ideally, defence organizations seeking to remain adaptive and agile could leverage the experience and expertise of private sector partners. The concept of an 'adaptive armed forces' goes further than traditional partnering. It aspires to deepen integration and embed private sector personnel and materiel resources securely within defence organizations to contribute to their operational capabilities. The Dutch have already expanded their network of reserve forces, streamlined the process for temporary hires, and expanded exchanges of personnel between defence, business, and other organizations.[9] A risk, however, is that external specialists employed on a temporary basis, or as reserve personnel, may come from companies that have a financial interest in securing future defence contracts. Any conflicts of interest that emerge in hiring, or in the bidding/contracting process, could seriously damage trust in defence institutions. Moreover, building more intimate business relations raises the risk of unfair competition and market distortions as industry partners gain competitive advantage. So, as militaries seek 'the right balance between owning ['make'] and being able to access certain capability ['buy'],'[10] they must also include integrity risk assessments. As armed forces increasingly embrace public-private partnerships, it is imperative that integrity-related risks are properly identified, mapped, and mitigated early on, and continuously reassessed.

[6] Note: The U.S. Commission on Wartime Contracting highlighted procurement process issues in conflict zones led to 'over-spending on contracts as a key concern.' It is also reported '…managerial shortages [in contracting expertise] and limited oversight of contractors…' as critical flaws in the procurement process. Mark Schwartz and Jack Swain, "DoD Contractors in Afghanistan and Iraq," *Congressional Research Service*, R40764, p. 3.

[7] United Nations Commission on International Trade Law (UNCITRAL), *UNCITRAL Model Law on Public Procurement*, January 2011.

[8] *Congresverslag Van defensief naar adaptief: Verslaglegging, toespraken en meer…* ('Congresverslag 2017'), Netherlands Ministry of Defence, 15 June 2017, p.; 'Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2017', *Kamerstuk 34 550 X, nr. 73, vergaderjaar 2016–2017,* Netherlands Ministry of Defence, 13 January 2017. In the United Kingdom, the concept of 'Whole Force' is similar to the Dutch commitment to having adaptive armed forces. Within the UK armed forces, sponsored reserves are personnel that are contracted through the private sector. See: Sir Nicholas Carter, "The UK perspective on the Adaptive Force," in *Congresverslag Van defensief naar adaptief: Verslaglegging, toespraken en meer…* ('Congresverslag 2017'), Netherlands Ministry of Defence, 15 June 2017, p. 23.

[9] Defence Vision 2035: 28. See also Defence Industry Strategy: 40; Congresverslag 2017: 21.

[10] Defence Vision 2035: 28.

Many PPP agreements involve financing, design, construction (or rehabilitation), together with service delivery over extended periods. Therein lies a risk. Complex and uncertain arrangements that require 'specific asset'[11] investments are often governed by incomplete contracts that cannot specify all future contingencies.[12] This forces public and private partners to cooperate closely and occasionally adjust payments, service provision, and other contractual obligations and performance goals as the project proceeds. The challenge is to properly evaluate and plan to address contingencies and risks that may arise during the life of the contract. This uncertainty makes PPP contracts vulnerable to later renegotiation. The greater the complexity and length of the contract, and the greater uncertainty in terms of future requirements, the greater the likelihood of renegotiation.[13]

Transparency in terms of sharing information in a PPP is essential to its success. Information the public partner provides to the private sector forms the basis of the PPP competition, while the information that companies share with the public sector forms the basis of their competitiveness in the selection process. However, the information asymmetry between private and public partners poses a dual risk, especially with incomplete contracts. On the one hand, companies may be tempted to exploit their information advantage in negotiations with the military through 'incomplete or distorted disclosure of information, especially calculated [or corrupt] efforts to mislead, distort, disguise, obfuscate or otherwise confuse.'[14] On the other hand, PPPs tend to increase the discretion of contracting authorities, raising the potential for 'abuse of public positions for private gain',[15]a standard definition of public corruption. Combined with a lack of transparency due to military secrecy, companies' resistance to disclosing information and the possibility of the abuse of increased discretion on the part of contracting authorities, can result in higher costs, lower quality, dangerous delays, and corruption risks.

PPP Risks: Insights from Transaction Cost Economics

In evaluating PPPs, two costs typically influence make-or-buy decisions: production costs, and the costs of designing, managing, motivating, and monitoring transactions or 'transaction costs.'[16] A NATO study finds 'setting up complex [PPP] arrangements is often very time-consuming and the overall set-up costs can exceed 10% of the capital value of the project.'[17] In evaluating the total costs of a PPP it is critical not only to estimate total system life-cycle costs (research and development, procurement, personnel, facilities, operations and maintenance costs, etc.). It is also necessary to get to grips with transaction costs (search and information costs; analysis and decision costs; and the costs of writing, negotiating, managing, monitoring, and enforcing complex long-term contracts).[18]

Transaction costs also include the risk of 'hold-up.' As the military increasingly relies on a company and its specific investments that benefit the partnership, these investments and the company's asymmetric information

[11] Examples of specific asset investments include: physical asset specificity with investments in excess capacity or specialized facilities, tools or equipment; human asset specificity with investments in specialized skills, knowledge, or training; and site specificity with investments in location of equipment, facilities, supplies, etc. that economize on transportation or inventory costs.

[12] For example: the risk of significant cuts/increases in military demand for a product or service due to changes in the threat environment, or due to political elections or bureaucratic turnover; or alternatively, supply chain issues impacting a private partner's ability to deliver agreed quantity or quality of products or services, or to respect promised schedules, or unanticipated impacts on supply chains (transportation, sub-contractors, etc.) or on inputs such as fuel, or other unanticipated cost increases; etc.

[13] Note that renegotiations of significant aspects of a PPP are in principle forbidden under EU law, subject to certain exceptions when: i) modifications have been provided for in the initial concession document; ii) additional works or services are necessary and cannot be provided by a new private partner for valid economic and technical reasons; or iii) a new private partner would impose significant inconvenience or substantial duplication of costs, and modifications are not substantial. (See European Commission, "Concession Contracts—partnerships between the public sector and a private company," downloaded 15 December 2021, https://ec.europa.eu/growth/single-market/public-procurement/legal-rules-and-implementation/concession-contracts_en).

[14] O. Williamson, *The Economic Institutions of Capitalism* (New York, NY: The Free Press, 1985).

[15] J. Svensson, "Eight questions about corruption," *Journal of Economic Perspectives* 19, no. 3 (2005): 19-42.

[16] R. Franck and F. Melese, "Defence Acquisition: New Insights from Transaction Cost Economics," *Defense & Security Analysis* 24, no. 2 (2008): 107–128.

[17] A. Altomonte et al., "Public Private Partnership in a NATO Context," Report STO-TR-SAS-112, NATO Science & Technology Organization, 2019, p. ES-1.

[18] Transaction costs are especially important in complex U.S. major defence acquisitions. For example, the Department of Defense employs an acquisition workforce of over 150,000 people, together with a USD 1 billion Defense Contract Management Agency (DCMA) with over 11,000 civilians and 550 military responsible for overseeing nearly 300,000 defence contracts valued over USD 7 trillion dollars. (See https://www.dcma.mil/About-Us/, accessed February 23, 2026).

advantage can increase switching costs. This places the private partner in a monopoly position to possibly 'hold up' the government at a later date, charging high prices for minor modifications (or 'change orders') to the original contract.[19] Valuable specific asset investments made by the private partner also tend to favour that company in any renegotiations, and can make it prohibitively costly for other companies to compete in subsequent re-bidding of the contract.

Interestingly, a 'hold-up' can also work the other way. Once a company has made/sunk substantial specific investments that have less value outside the partnership, the government could later change the terms of the contract to its benefit. An example is the case of U.S. military housing PPPs. Companies throughout the U.S. made significant long-run investments to build and operate military base housing. These specific asset investments depended on government payments of military housing allowances (BAH) that would guarantee a return on their investments. In their search for savings, Congress later lowered BAH payments, ignoring the private partners' fixed investments (sunk costs). [See Box 11.2]

Box 11.2: Military Housing PPP Case Study[20]

(An Example of Government 'Hold-up')

Today, PPPs own and operate 99% of military housing on U.S. installations across the country. In the early 1990s, the Department of Defense (DoD) struggled with deteriorating housing for its enlisted military personnel and their families, creating significant issues for retention, recruitment, and readiness. Faced with overwhelming funding (re-capitalization) needs, the DoD established PPPs with companies to update and build new housing, and to assume responsibility for family housing on military installations across the country. Congress enabled that transition in 1996 by turning its military housing over to the private sector (e.g. through the Military Housing Privatization Initiative, MPHI-10 USC 2871, provision in the 1996 National Defence Authorization Act, NDAA). This remains the largest PPP within the U.S. federal government.[21] More than USD 30 billion has been invested by private sector partners into U.S. military housing PPPs.[22] This includes roughly USD 8 of private investment for every USD 1 of public investment, leveraging USD 4 billion in government funding into more than USD32 billion in private funding for a portfolio of over 200,000 homes. The government established long-term (up to 50-year) partnership agreements with private developers to finance, build and manage military housing assets.[23] The private partners use rental revenues to pay operating expenses, make loan/bond payments, and capital (repair and replacement) improvements. The companies based their financial plans and bond sales to finance construction and renovations over the life of the PPP on forecasts of a benefit provided to military personnel called the Basic Allowance for Housing (BAH). While this PPP is one of the most successful to date, in a search for savings in 2015 Congress changed the terms of agreements between the government and private sector in its Fiscal Year 2015 NDAA, reducing the percentage of BAH paid to private partners. Reducing BAH lowered the revenue available for debt payments, operations and maintenance, and recapitalization accounts (to perform ongoing major renovations of homes). As a result, many military housing projects risked going into default, and along with deferred maintenance, this ultimately reduced the quality of military housing. Recognizing these risks, Congress later reversed its reductions to BAH

[19] This can arise when the military becomes dependent on a private company that has made specific (or corrupt) investments that make it indispensable, and where service disruptions have costly consequences. The partner may legally lock in the government by investing in productive 'specific assets' that increase performance, speed up schedules, or lower costs; or illegally through strategic bribes and favours.
[20] Additional details can be found in: Matthew C. Godfrey and Paul Sadin, *Privatizing Military Housing: A History of the U.S. Army's Residential Communities Initiative, 1995–2010, prepared for the Office of the Assistant Secretary of the Army, Installations, Energy & Environment* (Washington, D.C.: Government Printing Office, 2012). Evaluation of the Department of Defense's Implementation of Oversight Provisions of Privatized Military Housing, DODIG-2022-004, U.S. Department of Defense Inspector General, 21 October 2021.
[21] The Army calls their programme the Residential Communities Initiative (RCI). The Navy calls their programme Public Private Venture (PPV), while the Air Force uses Housing Privatization (HP).
[22] To leverage private debt and capital, MHPI established Limited Liability Companies (LLC/LP) where the Private Sector Partner serves as the majority managing member ensuring performance objectives are met. The Military Services generally serve as the minority member.
[23] DoD out-leases assets and land for 50 years with a twenty-five-year option under a Ground Lease, and transfers ownership of housing and improvements to the MHPI Partner Company.

in the Fiscal Year 2019 NDAA. However, since there is no guarantee this policy shift might not once again be reversed by Congress, this increases uncertainty and raises risks for private partners, potentially limiting future investments in military housing PPPs.

Hold up risks can affect either party in a PPP. Where the risk is that governments could hold up a private partner, companies may require credible commitments (government posting a bond, multiyear funding, etc.), or for the government itself to make specific investments that benefit the partnership: e.g. Government Furnished Equipment (GFE); or Government Owned Contractor Operated facilities (GOCO). But to ensure the private party makes appropriate use of government-provided equipment, facilities, etc., requires careful planning and effective control mechanisms.[24]

PPP Risks: Procurement Challenges[25]

A typical PPP procurement consists of three phases: pre-award, award, and post-award. (NCMA, 2019) These include a pre-tendering 'political phase,' an administrative 'solicitation/tendering' phase, and the operational or 'implementation' phase.[26] The three phases cover specification of the product or service, issuance of the solicitation (e.g. a Request for Proposal, RFP), the evaluation of proposals, award of the contract, implementation of the contract, and finally, the inspection and acceptance of delivered products or services. Each step is subject to risks.

The political phase can be subject to legal and illegal influence as defence companies try to persuade politicians to open up specific military projects or activities to PPPs. Meanwhile, politicians may be tempted to use PPPs to circumvent fiscal constraints by not including future PPP liabilities in national accounts.

The pre-award phase involves planning the procurement strategy, developing the solicitation document, and issuing the solicitation.[27] When a PPP concept is first market tested with potential bidders this opens opportunities for improper conversations or influence between bidders and government officials. Since many PPPs involve infrequent, lengthy projects with potentially lucrative returns, there can be perverse incentives for competing companies to win at any cost, including through deceptive and dishonest practices. Companies often attempt to influence the political and bureaucratic process through legal lobbying. However, in the absence of strict controls, this risks spilling over to illegal bribes or favours.

The bid solicitation process examines the extent of competition, establishes evaluation criteria and determines contract terms and conditions. Once the solicitation document is developed, it is then advertised in the marketplace.[28] Administrative tendering steps typically include: prequalification of companies,[29] development of technical evaluation criteria and their weights, agreement on post-award adjustments, and judging competitors. The source selection process may also include vendor negotiations and finally, selection of the contractor and award of the contract. [30]

[24] Note that governments may play different roles in the fight against corruption: as customer, regulator, and occasionally owner of equipment, facilities, or even industries involved in a PPP.
[25] This section relies heavily on J. Rendon and R. Rendon, "Analyzing procurement fraud in the US Navy," *Journal of Financial Crime* 29 (2022), 1297–1317. https://doi.org/10.1108/JFC-09-2021-0207.
[26] See R. Schomaker, "Conceptualizing Corruption in Public Private Partnerships," *Public Organization Review* 20 (2020): 807-820.
[27] Procurement planning includes analyzing products and/or services to be procured, analyzing the marketplace to determine industry's capability to produce or deliver the requirement, and developing statements of work and specifications.
[28] National Contract Management Association (NCMA), *Contract management standard (CMS) ANSI/NCMA ASD1-2019*, (Ashburn, VA: NCMA, 2019).
[29] PPP procurement is often broken into two steps, a qualifying step and then a bidding step. The qualifying step is where qualified bidders are identified, and the number of overall bidders invited to bid on the contract may be narrowed. The bidding step allows pre-qualified bidders to compete for the contract.
[30] So-called 'dialogue-based' PPP procurements may include two steps where technical specifications and characteristics of the product/service are discussed with preselected bidders, and where only bidders having passed the technical evaluation are authorized to submit a financial bid. The winning bidder is selected based on the best composite score aggregating the technical and financial evaluation.

In the award phase proposals are evaluated based on the evaluation criteria specified in the solicitation. It is helpful for evaluation criteria (weights and measures) to be independently reviewed as they can easily be manipulated to favour certain bidders. A transparent system that reviews and evaluates bidders and their bids based only on the merits of their proposal, can help ensure a PPP contract is correctly awarded to the private partner judged to have submitted the best offer.

Following the award of a PPP to a private partner, implementation steps typically include: vendor payments; performance (quality, cost, schedule) evaluation; and contract closeout or renegotiation. This post-award implementation phase requires monitoring the contractor's performance in accordance with the statement of work and specifications. It also includes inspecting and accepting contractor deliverables and managing the contractor payment process. When the performance requirements of the contract have been completed and accepted, the final step is the contract closeout process. Contract closeout involves activities, such as making final contractor payments and assessing and documenting contractor performance.[31]

Each phase and every step is susceptible to corruption and can lead to: inefficient vendor selection; inefficient service delivery; and increased operating costs. A detailed report on a major U.S. Navy fraud investigation reveals how each of these may have impacted the fleet.[32]

Procurement fraud can involve conflicts of interest, bribes and kickbacks, unjustified sole source awards, phantom vendors, leaking of bid data, unnecessary purchases, and unapproved product substitution. Collusive bidding by contractors and bid rigging schemes can exclude qualified bidders by leaking bid data, manipulating bids, and rigging specifications. Corrupt billing, cost, and pricing schemes can involve manipulating cost data, defective pricing, change order abuse, comingling of contracts, false, inflated, or duplicate invoices, and false statements and claims.[33] Fraudulent purchases include purchases for personal use or resale, unnecessary purchases, etc. Fraudulent representation may involve attempts by contractors to deliver supplies or services that do not conform or that fail to meet contract specifications, or involve unapproved product substitution.[34]

Conclusion: Reducing Corruption Risks

A well-integrated public-private defence industrial base is essential for the collective security of NATO Allies and partners. PPPs have the potential to leverage new technologies, financial and human resources, and infrastructure and equipment, from both the public and private sector to build a stronger foundation for the Alliance. However, corruption-related risks need to be addressed early in the procurement process.

To reduce these risks, it is helpful to establish a culture that emphasizes integrity, transparency, and accountability. This may require additional training, establishing specific procurement authorities, ensuring independent reviews and separation of procurement duties, preventing conflicts of interests, and documenting standard operating procedures. It may also require improving internal controls to ensure processes and activities align with organizational objectives and are in compliance with applicable laws and regulations, while promoting operational efficiency and effectiveness.

Empirical evidence suggests the risk of extortion or bribes and other collusion with public officials frequently occurs at the outset of a procurement. Or it might occur later, when the private sector partner is underperforming and unfairly seeks adjustments to performance requirements, attempts to distort invoices, or

Due to elevated corruption risks with open dialogue, governments should tightly control interactions between contracting authorities and bidders, and focus the dialogue only on technical aspects (which may include certain financial requirements) of the PPP. The contracting authority should also verify the accuracy of the relevant pre-qualification information provided by the winning bidder, 'Contract management standard (CMS)'.

[31] See footnote 26.

[32] See footnote 23.

[33] Association of Certified Fraud Examiners, *Report to the nations: 2020 global study on occupational fraud and abuse*, (Austin, TX: 2020): https://legacy.acfe.com/report-to-the-nations/2020/.

[34] Association of Certified Fraud Examiners*, Fraud Examiner's Manual* (Austin, Texas, 2012), p. 1.1423.

to alter regulatory and reporting procedures.[35] A successful PPP requires agreement on information disclosure, auditing, and dispute settlement mechanisms, and early awareness of corruption vulnerabilities. PPPs require ethical leadership, impartiality, strong institutions (competitive markets, clear rules and regulations, a competent legal/judicial system) and effective oversight (measurement, monitoring/audit, and enforcement capabilities).

Credible long-term PPP agreements are more likely when both sides have a culture and reputation for integrity in following through on their commitments. Reputations based on ethical norms and values and limited conflicts of interest are of pivotal importance when it comes to balancing control while establishing trust to reduce transaction costs and corruption risks. While reputations for *integrity* can build trust between public and private partners, the probability of success of a PPP also depends on consistent, competent and ethical management, systematic training, and cost-effective investments increasingly involving AI to increase *transparency* and improve *accountability*.[36]

Integrity: Public and private sector participants in a PPP procurement process should endorse and/or commit to complying with all domestic and applicable international laws, regulations and codes of conduct relating to anti-corruption.[37] Private sector companies bidding for PPPs should have their own published code of ethics and internal anticorruption procedures that can be independently audited. Governments should be particularly aware of conflicts of interest that might arise as the result of profit incentives, political or national affinity, family ties, or any other relevant connection or shared interests. Private consultants and experts should be independent with no conflicts of interest and a high level of integrity and competence to handle each stage of the project or tender. Responsibilities for preparation, evaluation, awarding and decision making in a PPP procurement should be divided and administered with clear authority, competency, scope of decision making, and/or dispute resolution assigned.

Transparency: To ensure a fair and transparent bidding process while promoting a competitive environment, PPP procurement requires fair and transparent communications with all potential bidders. It also requires minimum necessary and clearly communicated rules and regulations.[38] An independent anti-corruption authority can provide oversight, guidance, administration and enforcement in anti-corruption systems. Public disclosure rules are essential to promoting transparency in the PPP process. Recognizing secrecy requirements, governments nevertheless should institute robust disclosure practices to the extent possible at the outset of a PPP programme. Governments are challenged to recognize that projects involving assets of particularly high value, complexity, or political sensitivity may require additional mechanisms to ensure protection against corrupt practices. The PPP Evaluation Committee should have a clear threshold for decision making (e.g. simple majority, highest score, etc.), and make all decisions based on objective criteria, only using information derived from bidding materials and bidder responses over the course of the PPP procurement process. Oversight systems should be established to enable effective reviews of private partner activities, that they can endure and adapt to the substantial length of many PPP projects, and track the range and complexity of performance and payment activities undertaken in PPPs. Independent inspectors can audit the process to certify that the PPP process complies with applicable laws and regulations. Records management systems can provide comprehensive project tracking and record keeping, facilitate performance monitoring and management, retention of project documentation and materials, control billing and payment practices, while providing transparent and traceable contract administration records.

---

[35] Transparency International, *Curbing Corruption in Public Procurement: A Practical Guide,* July 24, 2014.

[36] The following is partly derived from work by Transparency International. (For example: Transparency International, *Handbook—Curbing Corruption in Public Procurement* (2006), https://www.transparency.org/en/publications/handbook-for-curbing-corruption-in-public-procurement; United Nations Economic Commission for Europe (UNECE) Working Party on Public-Private Partnerships, "Zero Tolerance Approach to Corruption in PPP Procurement" (Draft v2.0; Action: Revised draft; Status: Draft v2.0; based on an initial draft prepared by an international project team led by Marc Frilet, March 2017), https://wiki.unece.org/download/attachments/23758445/PPP%20Zero%20Tolerance%20approach%20to%20Corruption%20in%20PPP%20Procurement%20Project-Public%20Review%20v2.0.docx?version=1&modificationDate=1489143144877&api=v2.

[37] Transparency International, "The Integrity Pact—A powerful tool for clean bidding," January 2009, https://baselgovernance.org/publications/integrity-pact-powerful-tool-clean-bidding.

[38] An important caveat is that Transparency International and others have identified excessive rules and regulations as contributing to corruption. See, for example, Transparency International, "Reducing bureaucracy and corruption affecting small and medium enterprises," https://knowledgehub.transparency.org/helpdesk/reducing-bureaucracy-and-corruption-affecting-small-and-medium-enterprises.

Performance monitoring can assist in managing the partner and project and in identifying any necessary project modifications and/or performance adjustments.

Accountability: Violations of the law, rules, regulations, or codes of conduct relating to anti-corruption need to be enforced and punishable with fines, civil or criminal penalties, and the removal or disbarment of offending persons or businesses. Governments should establish whistle-blowing policies, rules, regulations and procedural frameworks easy to initiate by a whistle-blower, that protect recognized whistle-blowers to enable and encourage proactive disclosure of conflicts, corrupt manipulation, and other fraudulent practices.

Reducing corruption risks not only depends on the careful governance of PPPs, but also on the integrity of public officials and private partners, and the transparency and accountability of military governance mechanisms and institutions. A carefully developed country-specific mix of integrity, transparency, and accountability policies can reduce the risk of corruption that might otherwise undermine the benefits of PPPs.

Part 4: Players in Building Integrity

Part Four examines the actors who stand outside defence institutions yet profoundly shape their integrity. The first chapter shows how parliaments conduct oversight through budget authority and scrutiny to reduce corruption risks, protect national resources, and hold defence institutions accountable. The second chapter explores anti-corruption agencies, tracing their global rise, the standards that guide them, and their role in investigating corruption. It analyses the highly sensitive defence sector, where secrecy sometimes shields wrongdoing. Finally, this part highlights civil society as a vital partner in democratic defence governance, revealing how transparency organizations, watchdogs, and citizen groups press for accountability, participate in oversight, and support the reform process. Using the Government Defence Integrity Index as a lens, it shows how civil society contributes to oversight, exposes weaknesses, and strengthens trust between citizens and their armed forces. This part proves that integrity in defence is not given and that the quality of oversight depends on active CSOs, empowered legislative bodies, and engaged military institutions. Integrity is a shared act and a collective responsibility.

12. Parliaments: Using the Power of the Purse in Tackling Defence Corruption

Teodora Fuior

'The State will perish when the legislative power is more corrupt than the executive power.'

Montesquieu, 1748

The relationship between parliament and military budgets goes back many centuries. The slow emergence of representative assemblies in Europe, after the twelfth century, was triggered by the need for European monarchs to fund wars and seek help from representatives of different social classes, called to agree to additional taxation.[1] One of the fundamental principles of accountability, stating that *there should be no taxation without parliamentary consent*, became widely accepted in England during the fourteenth and fifteenth centuries. During that time, the House of Commons worked with monarchs not only to enlarge the nation's tax base, but also to remove incompetent or corrupt officials.[2] In Europe, England was the first to link three elements that are essential to nation building: the state, the rule of law and political accountability. This produced a state so powerful, legitimate, and favourable to economic growth that it became a model followed throughout the world.[3]

Today, all democratic constitutions entrust parliaments with what is called 'the power of the purse', defined as the ability to tax and spend public money on behalf of the national government. The control over budgets and taxation gives parliament institutional leverage in its relationship with the executive branch. The power of the purse lies at the foundation of the democratic checks and balances system, and is one of the main sources of parliamentary influence in politics.

In practice, the power of the purse means that constitutional and legal provisions guarantee the parliamentary approval of all fiscal matters, the most important of them being the annual State Budget. This grants members of parliament the right to access information on budget execution, actual expenditures, and audit reports. The annual State Budget is one of the most important policy statements of a government. It sets out how tax money and other state revenues are prioritized, allocated and spent by every state agency, including the defence and security sectors.

This chapter will explore the opportunities and means available to parliament to contribute to the integrity of the defence establishment, through an effective use of the power of the purse.

1. Making Defence Integrity a Priority for Parliament

Parliaments must ensure that the military and other security services occupy an appropriate place in the nation's priorities and are used for the political purposes expressed by citizens' representatives. Consequently, a fine balance must be kept between the effectiveness of these services and the extent of their democratic control: the security sector must be allocated sufficient powers and resources to enable them to provide security effectively. However, it must not absorb too many national resources, nor exert an excessive influence on the development of policy.

[1] King Edward I made the meeting of Parliament a frequent event. He summoned nobles and churchmen, and issued orders (known as 'writs') for the election of two representatives from each county (the knights of the shire) and two from each city or town (the burgesses) to attend. They were called on primarily to listen to and approve the King's plan for a new tax. It became an accepted rule that the representatives of those who were going to be most affected by taxation had to give their consent to it in Parliament. Over the course of Edward I's reign (1272-1307) he summoned Parliament regularly, on 46 occasions. From 1278, official records were kept of Parliament's proceedings and decisions, written up and sewn together in long scrolls, the Rolls of Parliament. 'Changes under Edward I,' https://www.parliament.uk/about/living-heritage/evolutionofparliament/originsofparliament/birthofparliament/overview/edward/.

[2] Francis Fukuyama, *The Origins of Political Order*, vol. 1 (London: Profile Books, 2011), p. 413.

[3] Ibidem, p.421.

Public trust in national armed forces is very high in many countries, often exceeding the trust placed in other institutions; something that can be observed consistently across different continents and political regimes.[4] Public surveys typically indicate that the military is one of the most respected institutions in society, enjoying much more public confidence than government, media, private sector, parliament and political parties. However, various studies rate defence as one of the most corrupt areas of government activity.[5] Corruption in defence may take many forms, including kickbacks and bribes, single source or non-competitive procurement contracts, manipulation of soldier payrolls, misuse of budgets, and the use of military resources to generate off-budget profits.[6] Defence corruption undermines the ability of defence forces to fulfil their core mission, and 'in the worst cases it has the potential to exacerbate conflict rather than to respond to it effectively.'[7]

The integrity of the defence establishment should be a priority for parliaments, for several reasons.

Resources allocated to defence are significant in size and are ultimately diverted from other sectors of public life, such as education, healthcare, innovation and development. Defence and security budgets represent a large proportion of public budgets, and the security sector is an important (often the largest) state employer in the national economy. When resources allocated to defence are not effectively and efficiently spent the national defence capacity is diminished. Defence corruption has a negative impact on soldiers' safety and morale, on training and combat preparedness; it may also contribute to the criminalization of the national economy and politics. It, after all, allows criminal and hostile foreign groups to acquire national information, know-how, dangerous materials and weapons technology. It is the responsibility of parliaments to safeguard the integrity of the defence sector and ensure that governments are good employers in terms of safe working conditions, regular payment of salaries and pensions, as these are building blocks of national defence capacity and resilience. Defence sector corruption undermines public confidence in the state. It leads to a loss of public trust in the military and in government, undermining the nation's defence readiness, social cohesion and international reputation. Accounts of corruption associated with defence and security contracts frequently make it to the front page of newspapers around the world.

Playing a meaningful role in defence and security policy and making sure that the defence establishment functions with effectiveness and efficiency is not an easy task for parliament. The first big challenge is the asymmetry of information and expertise that exists between parliament and the defence establishment. Members of parliament (MPs) and parliamentary committees are often dependent on the government's monopoly on defence related information. They must invest time and effort in developing in-house expertise (MPs, professional staff assisting committees, parliamentary research services). They must create a reliable

[4] See, for example, Courtney Johnson, "Trust in the military exceeds trust in other institutions in Western Europe and U.S." Pew Research Center, September 4, 2018, https://www.pewresearch.org/short-reads/2018/09/04/trust-in-the-military-exceeds-trust-in-other-institutions-in-western-europe-and-u-s/; Gallup, "Confidence in Institutions," https://news.gallup.com/poll/1597/confidence-institutions.aspx.; Clancy Bertane, "National Governments Get Low Marks in the EU," Gallup, December 22, 2011, https://news.gallup.com/poll/151715/national-governments-low-marks.aspx.

[5] 62% of the 86 assessed countries face a high to critical risk of corruption in their defence and security sectors, almost all countries have poor safeguards against corruption in military operations, while 86% of global arms exports and 49% of global arms imports originate from, or are sold to countries facing a high risk of defence corruption. Press Release, *Transparency International*, November 16, 2021, https://www.transparency.org/en/press/62-per-cent-countries-at-high-risk-of-defence-and-security-corruption. Transparency International Global Bribe Payers Index 2006 rated the defence sector as one of the top three sectors for bribery and corruption, along with the oil sector and major infrastructure projects.
The IMF report on corruption and military spending explains, 'Procurement is an important channel through which corruption affects military expenditures.' Moreover, according to the same report 'bribes account for as much as 15% of the total spending on weapons acquisition', Sanjeev Gupta, Luiz de Mello, and Raju Sharan, *Corruption and Military Spending*, WP/00/23, International Monetary Fund, February 2000, https://www.imf.org/external/pubs/ft/wp/2000/wp0023.pdf. The U.S. Department of Commerce estimates that 50% of all bribes in global transactions are paid for defence contracts; numerous single source defence contracts have been awarded for operations in Iraq. See Mark Pyman, Regina Wilson, and Dominic Scott, "The Extent of Single Sourcing in Defence Procurement and its Relevance as a Corruption Risk: A First Look," *Defence and Peace Economics* 20, no. 3 (2009): 215-232at p. 217.

[6] Todor Tagarev, ed., *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices* (Geneva: NATO/DCAF, 2010), https://www.nato.int/cps/en/natohq/topics_104893.htm.

[7] Natalie Hogg, statement in '62% of countries at high risk of defence and security corruption, index reveals,' Press Release, *Transparency International*, November 16, 2021, https://www.transparency.org/en/press/62-per-cent-countries-at-high-risk-of-defence-and-security-corruption.

network of external allies in specialized institutions such as the National Audit Office, in academia and civil society, in order to get access to independent analysis and information about defence matters.

2. Understanding Why the Defence Budget is Different

The security sector is, in principle, subject to the same broad set of rules and procedures that apply to other sectors of government activity. Budgeting for security should not be different, nor should it be less transparent. However, the complexity and specificity of the security sector complicate the involvement of national parliaments in the analysis and oversight of the defence budgeting process. Security is not only a public good. It is the *most* important public good, because it enables the state to provide for citizens' access to other public goods, such as personal freedom, social justice, prosperity, education, and health.

A distinctive feature of defence budgeting is the accentuated **political nature** of this process. How much a country spends on security, and on what, are political decisions that inform domestic constituencies, neighbouring states, regional and international actors about the perception of threat in a society and the government's intentions in security matters. Defence and security spending have great consequences for national industries and employment, and may aggravate nationalistic feelings, and regional discrepancies or ethnic rivalries.

Budgeting for defence and security is also a **foreign policy instrument.** It sends early signals to other states about a country's strategic priorities and future intentions. Variations in the size and composition of defence budgets are closely monitored internationally and often influence the behaviour of both partners and competitors. Increases in defence spending can likewise serve to reassure allies and strengthen collective commitments — as illustrated by NATO Allies' 2025 pledge to move toward defence expenditures of up to 5% of GDP.

Unlike most other public policies, the efficiency of a country's defence and security policy is oftentimes difficult to measure. The absence of clear-cut **performance indicators** makes the analysis of defence spending a challenging task. How many soldiers, what sorts of weapon systems or how much readiness should the defence establishment provide to be effective? How should one evaluate whether defence capacities perform in wartime as they were projected to perform in peacetime exercises?

In most countries the security sector is continually reforming itself and adapting to new security risks and threats. Another distinctive feature that must be considered before analysing the details of a yearly defence budget is that security and defence policies are developed through long-term planning and reforms, with **multi-year programmes**.

Additionally, the need to protect **sensitive national security information** frequently prevents transparency and accountability mechanisms from functioning in the same way as they do for other public policies. Secret programmes (that may be included in budgetary documents, but not detailed, nor clearly identified) are often used for defence research, development, acquisition, military operations, and intelligence activities. The identity, purpose and even costs of covert operations are concealed from the public, but also from most members of parliament. They are protected by security protocols that limit access to sensitive information to only authoriZed officials. Therefore, parliament must prevent the executive from over-classifying information without solid justification. Mechanisms for allowing access to classified information for selected members of parliament are in place in all democracies to ensure that some degree of accountability exists even for classified programmes and budgets. In line with the principles of transparency and accountability, the circumstances and conditions of how this classified information can be accessed must be clearly defined by law and rules of procedure and also shared with the public.

Box 12.1: Black Budgets in the United States

Special access programmes (SAP) and special access budgets (SAB) are the Pentagon's official terminology for respectively 'black programmes' and 'black budgets'. The authorization for SAP is granted by the President. Not more than 1% of representatives receive information about the content of 'black budgets'.

Among 'black programmes', further distinction is made for 'waived' programmes, considered to be so sensitive that they are exempt from standard reporting requirements to Congress. Only eight members of Congress (the chairs and ranking members of the four intelligence and defence committees from the House of Representatives and the Senate), the so called 'Gang of eight' are orally notified of the existence of a waived programme, without being given any further information about it. This enables them to truthfully declare no knowledge of such a programme if asked by the public, thereby maintaining secrecy. A programme which is 'black', waived and unacknowledged is 'deep black'. The most secret of the intelligence and covert operations conducted by the CIA are 'deep black'.

3. The Difference between Defence Budgets and Military Expenditures

'Defence budget' and 'military expenditures' are the most common terms in public debates on budgetary issues concerning the security sector. They usually cover the largest part of security sector expenditures. However, the terms refer to different things. The 'defence budget' is the official data provided by governments under the budget of their ministry of defence (MoD).

'Military expenditures' are the total annual cost of maintaining the defence establishment. Military expenditures usually add to defence budgeting lines from non-defence ministries, received foreign military aid and other off-budget military spending. For example, military construction, arms procurement, military pensions, received military aid and paramilitary forces may be listed as part of the budget of ministries or state agencies responsible for development, economy, social security or internal affairs. These expenditures can be sometimes difficult to identify, because they are lumped together with non-military expenditures. Sometimes there is a deliberate attempt to conceal such items in non-defence budget accounts.

Extra-budgetary expenditures can also cause military expenditures to skyrocket. OECD defines off-budget funds as -special funds owned by the government, that are not part of the budget and that receive revenues from earmarked levies, possibly next to other sources such as fees and contributions from the general tax fund.[8] In many African, Latin American or Asian countries, the military possesses large income sources such as state-owned companies, commercial activities and the exploitation of natural resources that fall outside the official budget. This income cushions the personal salaries of high-ranking military officers and funds arms purchases among other collective expenditures. Enabling the military to dispose of extra-budgetary resources allows a substantive bandwidth to spend without accountability to a third party.

Debt incurred by military purchases further complicates the accurate measurement of a country's total defence expenditures. Imports of military equipment financed by foreign loans create an economic burden. The interest and amortization payments incurred by the imports are extremely difficult to depict in state budget documents. Additionally, so-called 'black budgets' – funding secret operations authorized by the executive – are a type of 'blank check' that the government can request from parliament. Few members of parliament receive information about the content of these budgets (see Box 12.1), and it is impossible for independent experts to analyse or criticize their content.

[8] Organisation for Economic Cooperation and Development (OECD), *Glossary of Key Terms for completing the 2012 OECD Budgeting Practices and Procedures Survey*, (Paris: OECD), https://www.oecd.org/gov/budgeting/Budgeting-survey-glossary.pdf.

Box 12.2. What Does the Term 'Defence Budget' Stand for?[9]

Expenditures **usually included** in the 'defence budget,' –the MoD budget:

- Personnel (all expenditures on current personnel, military and civil: salaries, food, social services for personnel and their families);
- Operations and maintenance;
- Arms procurement;
- Military research and development;
- Military aid (appears in the budget of the donor country).

Expenditures **frequently excluded** from the 'defence budget' – the budget of other ministries and agencies, plus off-budget expenditures:

- Civil defence;
- Economic defence (protection of strategic infrastructure, oil reserves, food supplies etc.);
- Psychological defence (from hostile enemy propaganda);
- Current expenditure for past military activities (can appear in the budget of various non-defence ministries);
- Veterans' benefits;
- Demobilization and reintegration programmes;
- Conversion of arms production facilities;
- Destruction of weapons;
- Defence expenditures placed under the ministry of interior budget lines (for paramilitary forces like Gendarmerie, Home Guards);
- Salaries for military personnel working on development projects (such as building roads);
- Military construction (can appear in the budget of the development ministry!);
- Foreign military aid (does not appear in the budget of the receiver country!);
- Revenues from economic activities of the armed forces;
- Conversion of defence facilities through privatization, sale or rent;
- Access to and exploitation of natural resources by the military;
- Military commercial activities (sometimes exempt from taxation);
- Debts incurred by military purchases (interest and amortization of military equipment financed *via* foreign loans);
- Barter trade (commodities bartered for military equipment);
- Contingency funds and emergency funds (can sometimes appear only in budget rectification or supplementation).

'Black Budgets': the identity, purpose and cost of secret operations are not detailed or not clearly identified in budget documents but can be accessed by a restricted number of parliamentarians under certain conditions (as described above).

4. The Defence Budget Document

The presentation of budget documents tends to be complex, making the task of understanding the process a difficult one. The executive can submit its budget proposal to the national parliament in a variety of forms, at differently disaggregated levels of detail.

[9] Based on Dylan Hendrickson and Nicole Ball, *Off-budget Military Expenditure and Revenue: Issues and Perspectives for Donors* (London: King's College London, 2002), CSDG Occasional Paper no. 1. See also Survey on Budgeting Practices and Procedures, OECD, 2012, question 38a, https://www.oecd.org/gov/budgeting/2012-Budgeting-survey.pdf.

The size of the budget document can range from a few pages summarizing how funds are allocated between agencies, to hundreds of pages of exhaustive, complex breakdowns.

The budget document contains:[10]

- Fewer than 250 line-item appropriations in the UK, Austria, Netherlands, France, Canada and Poland.
- In Italy and Slovenia, the number of line-items has dropped from several thousands in 2007 to less than 500 in 2012.
- Line-item numbers are also slightly decreasing in Ireland, Israel, Czechia, Switzerland and Greece.
- In other countries, the number of line-items is increasing, reaching 1,500–2,000 in Norway, the U.S., Denmark, Belgium and Mexico.
- In several OECD countries the budget document provides thousands of line-items: like Germany (6,000), Spain (16,700), or Türkiye and Portugal with more than 40,000 line-items.

Appropriation titles are the most common form used in budget submissions, i.e. listing expenditures according to their objects. Major titles of a defence budget usually include Military Personnel, Operations and Maintenance, Procurement, Defence Conversion Programmes, and Research and Development. Appropriation titles are further subdivided into appropriation **accounts,** which are further disaggregated into budget **activities** and **line items**. The detail provided may vary from one title to another. The most important function of a line-item budget system is the specification of budget ceilings, which takes place during the allocation process and is meant to ensure that agencies do not exceed their allocated funds.

The strengths of **line-item budgeting** are relative simplicity, lack of ambiguity and the potential for control of expenditures through easy comparisons with prior years, using the detailed specification of inputs. On the downside, line-item budgeting does not provide sufficient information on the rationale of why money is being spent the way it is or on envisaged improvements in terms of effectiveness and efficiency in funds spending. It also tends to encourage short time horizons and the micromanagement of budget implementation. Therefore, line-item budgeting on its own is considered today by many countries 'an inadequate basis for allocating resources and controlling expenditures'.[11] The excessive abundance of line-items may constrain managerial flexibility and the capacity of the legislator to analyse and comprehend the budget document. NATO countries have installed a planning, programming and budgeting process system, which uses defence objectives as a starting point, and connects defence planning with defence budgeting. **Programme budgeting** has a multiyear focus and is conducive to 'output budgeting', involving costing out 'programmes' – public policy objectives – and the steps necessary to achieve those objectives. Budgets are developed around functional outputs or missions such as strategic forces, special operations, peacekeeping operations, communication systems and emergency aid, rather than around ministries or organizational units.

Programme budgeting helps illustrate the purposes for which money is being allocated, facilitates cost-benefit analyses of defence expenditures and links plans with funds as well as inputs with outputs. However, there are a number of limitations to programme budgeting: It is very difficult to leave the organizational focus of budgeting behind and budget solely on the basis of programmes. It is also difficult to compare programme spending in terms of effectiveness, and to make choices on that basis.

To level up the different weaknesses and strengths of these approaches in budgeting, in many countries the budget document presents information on both item and programme budgeting.

[10] Organisation for Economic Co-operation and Development (OECD), *Budgeting Practices and Procedures in OECD Countries* (Paris: OECD Publishing, 2014), p. 61, https://doi.org/10.1787/9789264059696-en. The Report compares the results of an OEDC survey conducted in, respectively 2012, and 2007.

[11] Organisation for Economic Co-operation and Development (OECD), *Budgeting and Public Expenditures in OECD Countries 2019* (Paris: OECD Publishing, 2019), p. 24, https://doi.org/10.1787/9789264307957-en.

5. The Defence Budgeting Cycle

The budget cycle is the time frame in which all major steps of a yearly budget are being developed: decision-making, implementation and assessment. Budget analysis should distinguish between the four main stages of the budget cycle: formulation, approval, execution, and evaluation (audit). At each stage, the roles and actors involved and their possibilities for evaluating and influencing the process are different.

One of the most comprehensive and detailed publicly available sources of information about procedures followed and practices developed throughout the budget cycle in different countries is provided by the OECD. The Budgeting Practices and Procedures Database[12] is the depository of detailed data on how budgets are handled in OECD countries from formulation to approval, execution and reporting, based on surveys conducted every four to five years. The Parliamentary Budgeting Practices[13] database was created based on a questionnaire sent out to OECD parliaments for the first time in 2012, then repeated in 2018. This database provides a unique set of information on national parliamentary budgeting practices from 34 OECD member countries, looking at the role of different chambers in budgeting, the work and the powers of committees, the analytical expert support available to different parliaments, the relationship between parliament and national audit office and public participation in the parliament's work related with the budget. Many of the assessments made in this chapter are based on information available in these databases.

The 2019 OECD report on Budgeting and Public Expenditures writes that 'while the budget approval phase is still where most legislatures come to the fore in the budget process, there is a trend away from treating the budget as a set-piece event towards continuous financial scrutiny throughout the year'.[14]

Budget Formulation

How the state budget is designed reflects the government's political choices and priorities for the future, and its implementation affects the lives of every citizen. Budget formulation is a process of negotiation within the executive on how the funds available for the next fiscal year should be distributed between and within ministries. Ministries and other state agencies submit their budget proposals to a central budget authority (usually the ministry of finance). The ministries formulate their budgetary needs, in line with the guidance provided by the government's national objectives, the specific objectives of the ministry and the input received from its different components. Each ministry usually seeks a larger budget, which the ministry of finance modifies according to fiscal limitations and national priorities. The adjustments made in this negotiation process depend not only on the funds available, but also on the relative leverage of the ministry of finance compared with the spending ministries. At the end of this process a budget is drafted, which, after being agreed upon by the executive, is submitted to parliament for final approval.

This stage of the budget cycle takes place mostly within the executive, behind closed doors, and in most countries without formal involvement from parliament. Still, parliamentary and public debates can influence political parties and executive entities in budget formulation. The more parliament is involved in the debate on security priorities and long-term defence planning (using plenary debates, questions and interpellations, committee hearings, motions etc.), the more influence parliament has on how the executive decides to shape the budget.

Lively parliamentary debates during budget formulation increase the transparency and the inclusiveness of the process. They give opportunities to civil society organizations and the larger public to be informed and to express their own preferences and alternative proposals.

[12] Organisation for Economic Co-operation and Development (OECD), O*ECD International Budget Practices and Procedures Database,* https://qdd.oecd.org/subject.aspx?Subject=BPP_2018.
[13] Organisation for Economic Co-operation and Development (OECD), *OECD Parliamentary Budgeting Practices Database* https://qdd.oecd.org/subject.aspx?Subject=PBO_2018.
[14] Organisation for Economic Co-operation and Development (OECD), *Budgeting and Public Expenditures*, p.82.

The yearly budget allocated to the defence and security sector must be embedded in a planning process that extends over several years. This process is usually laid out in public documents such as **national security strategies, white papers and defence policies** issued by the executive and agreed upon – or in many countries formally adopted – by the national parliament. They may refer specifically to the planned level of defence spending, personnel policy, arms acquisition and to levels of possible participation in peace support operations, if any. Therefore, **analysing these long-term planning documents is a prerequisite** to analysing the yearly budget allocated to the security sector. Parliamentary involvement in the approval of these documents and subsequent public debate is an essential preparatory step for the accountability of the yearly security budget.

Yearly budget formulation has two distinctive levels, which involve competition between different interests and agencies. First is the **setting of national priorities** (allocating resources *to* the security sector). Nations must spend their finite resources wisely and invest both in military capacities and civilian goods. This competition between 'funding guns or butter' is, in many countries, one of the most important subjects of budget analysis, for it can reveal the underfunding of civilian services and an over-militarization of foreign policy. Or, on the contrary, insufficient funds allocated to the security sector may create vulnerabilities, an incapacity of state institutions to ensure national defence, public order and security, jeopardizing the position of the state in the international system. Rectifying eventual imbalances can be addressed by parliament in this early stage of budget formulation.

Second, there is the setting of security priorities (allocating resources *within* the security sector). At this level of analysis, we see how the budgeting process is separating different agencies within the security sector, each and every one of them competing to get a bigger slice from the overall budget the country is willing to invest in 'guns'. How much they manage to get will affect their competitiveness in many ways, from their capacity to fulfil legal mandates and objectives to their attractiveness on the labour market. It is common to see how highly skilled employees migrate from one security service to another, as the capacity of these institutions to offer attractive salaries and working conditions fluctuates along with their budget. This is a non-exhaustive list of ministries and government agencies involved in the delivery of security services, whose budgets are the constituent parts of the overall defence and security budget:

1. **Defence**
    a. the armed forces–including peacekeeping forces deployed abroad;
    b. the civil administration of the military sector–defence ministry and other government agencies engaged in defence activities, such as arms production, imports and exports;
    c. paramilitary forces–non-regular armed forces which are to be trained, equipped and available for military operations, such as the *gendarmerie* or border guards (they may appear in the budget of defence or interior ministry).
2. **Law enforcement:**
    a. the police and other forces responsible for public order and law enforcement;
    b. the civilian administration of police and other public order forces (interior or home affairs ministry).
3. **Border management & customs:** border guards/police and customs administration.
4. **Corrections:** administration of prisons (this may appear in the budget of the interior or justice ministry).
5. **Intelligence:** a variety of agencies and departments perform intelligence activities, military and civilian, domestic and foreign; they may appear under the budget of the defence, interior, justice ministry, or as independent services.
6. **Civil emergencies:** agencies responsible for emergency situations, civil protection, special communications, strategic infrastructure protection, etc.
7. **Strategic management of security:** the Supreme Council for Defence or National Security Council, which may be an administrative independent institution, or an advisory department under the chief of the executive.

Box 12.3. Parliament Involvement in Budget Formulation[15]

An increasing number of parliaments debate the direction of fiscal policy and budget priorities before the annual budget is submitted for approval. Such debates are based on a pre-budget report submitted by government to the legislature.

- The Swedish Riksdag has a two-step budgetary process: the Spring Fiscal Policy Bill (submitted in April) allows for a general debate of fiscal policy, and the Budget Bill (submitted in September) presents the detailed spending proposals for the next year;
- The Czech Parliament's Budget Committee holds a pre-budget debate and passes a resolution on the budget strategy and convergence programme;
- The newly established Committee on Budget Oversight in Ireland holds pre-budget hearings on budgetary priorities and issues a report to the plenary;
- The Finance Committee in Israel has pre-budget debates in order to signal their preferences during budget formulation.

Parliaments, and especially defence and security committees have a key role to play in the allocation of resources within the security sector. They can ensure that the distribution of funds allows for a balanced development of capacities, aligned with national interests and priorities, providing a fair working environment for security employees. The most useful instruments that can unify and integrate these distinct functions and institutions are national security strategies and holistic security sector reforms.

Three general criteria should be observed in the parliamentary debate of budget formulation:

1. The funds allocated to the security sector should be accordant with **national interests**, based on the security agency's roles, missions, tasks, and the long-term costs incurred by long-term reforms and modernization projects.
2. Planned security expenditures should be affordable to **economic possibilities**; the long-term costs must be correlated with medium-term economic forecasts.
3. The financial burden of the security sector must be **acceptable to the respective societies** at large. Hence the importance of having these debates in parliament from the early stages of budget formulation.

Box 12.4. Methods to Determine Annual Expenditures for a Ministry

- Projected level of spending is correlated to the expenditures of the previous fiscal year;
- Level of spending is calculated as a percentage of the GDP;
- Level of spending may be subject to international agreements, e.g. NATO recommends members allocate 5% of their GDP to defence;
- Level of spending is correlated to foreign benchmarks, e.g. how much other countries spend for the same sector in absolute terms, per capita or as percentage of the GDP;
- Level of spending is determined exclusively in the context of new circumstances and agreed national priorities, as compared with other priorities (such as education or health care delivery).

[15] OECD, *Budgeting and Public Expenditures*, p.83.

Budget Approval

In the budget approval stage, parliament's power of the purse is on full display, as parliament reviews, amends, and enacts the budget proposal into law. Parliamentary authorization of all public spending and taxation represents the 'rule of law' in public finance and is one of the core principles of parliamentary democracy.

Parliament dedicates a significant amount of time each year to budget approval, usually one or two months. The OECD Best Practices for Budget Transparency recommend that the executive should submit its budget proposal to the legislature at least three months prior to the start of the fiscal year and that the legislature should approve the annual budget law prior to the start of the new fiscal year.[16]

The degree to which parliament can perform its role at this stage and use the 'power of the purse' depends on several factors:

- The timely submission of the budget proposal by the government, according to a predictable and transparent schedule – eventually set out by law;
- the quality and comprehensiveness of the information it receives (in the budget documents and during the hearings of budget holders);
- the time available for analysis, debate and vote;
- the actual authority to amend the budget (awarding extra funds or removing funding for a department or program).

Box 12.5. What Are the Consequences of the State Budget being a Law?

- Guarantees parliamentary participation in decision-making;
- It is a public document, available on the internet, in public libraries throughout the country and a useful basis for holding the government to account;
- Non-compliance with the budget law can be punished as a crime.

What are the differences between State Budget Law and ordinary laws?

- Only the government can formulate and submit the budget proposal;
- Parliamentary amendments are often limited by the necessity to indicate the source of funds for any desired increase of the budget;
- All sectoral committees are usually involved at the same time, sectoral committees providing opinions on the ministries in their competency and the budget committee in the lead for drafting the budget report;
- If parliament has more than one chamber, most often the upper chamber allocates much less time to budget debate and might have no power to amend or reject the budget. In the OECD only four countries report that the upper and the lower chamber have co-equal budgetary powers: Chile, Italy, Switzerland and the United States.

The essential indicator of parliamentary impact is the extent to which its amendment process influences the budget process. In broad terms, there are three models describing the legal powers held by parliament in the budget approval stage.[17]

[16] Organisation for Economic Co-operation and Development (OECD), *Best Practices for Parliaments in Budgeting*, GOV/SBO(2022)3 (Paris: OECD Public Governance Directorate, 2022). https://one.oecd.org/document/GOV/SBO(2022)3/en/pdf.
[17] OECD, *Budgeting and Public Expenditures*, pp. 88-89.

Unrestricted powers to amend the budget proposals and propose new expenditures. In theory, such powers of amendment empower parliament to rewrite the whole budget proposed by the government. The U.S. Congress is generally pointed to as the most illustrative example: the Executive proposal, formulated by the President, is really taken as a proposal, analysed and amended in detail by Congress. The German Bundestag, the Dutch and the Danish parliaments also initiate hundreds of budgetary amendments annually. Over half of OECD countries report unrestricted amendment power. For example, Austria, Belgium, Finland, Hungary, Norway and Portugal also enjoy unrestricted powers to amend the budget; however, in practice this formal power is little used.

Restricted powers allow parliament to amend the budget proposals, as long as amendments do not change the total deficit or surplus proposed by the executive. This allows parliament to change government priorities and, by re-allocating funds, to decide upon final budgeting priorities. The restriction to keep the total deficit unchanged is justified by the need to respect fiscal discipline and macro-economic indicators. Therefore, parliament has to indicate the source of funds for any increase of the budget by correspondingly decreasing other line items, or by establishing new sources to finance them. Otherwise, the electoral pressure to spend more and to tax less would generate chronic deficits. Parliaments in Czechia, France, Mexico, Poland, Spain and Romania follow this model.

Only a few parliaments are given **limited powers** to amend the budget proposals. Parliaments may be limited to only reducing existing expenditures, without reallocating those funds to other priorities. In some cases, they lack any authority to amend the budget and may only approve or reject it in full. This model is common in Commonwealth countries such as Canada, the UK, Australia, India, New Zealand, South Africa and Zambia. However, the lack of statutory power in budget approval is usually compensated by the vigilant involvement of parliament and other independent bodies (such as Supreme Audit Institutions) in other stages of the budgetary cycle.

Too often, regardless of parliament's legal power to change the budget proposals, the level of amendment in practice is extremely modest, granting the executive an almost-complete monopoly over determining the budget figures. There are two main explanations for this underuse of the 'power of the purse.' First, in many countries, notwithstanding the formal powers of the legislature to amend the budget, a vote on the budget is considered a vote of confidence in the government;[18] the significant time allocated to the budget, the mobilization of all parliamentary committees and resources and the public debates triggered by the budget are an important manifestation of the separation of powers and the democratic checks and balances, even in the absence of significant amendment. Second, the increased difficulty and complexity of the budgeting process is far from being matched by the parliamentary capacity to understand budget documents and to engage in a multi-year analysis of budget trends.

An increasing number of parliaments have specialized budget research units and a Parliamentary Budget Office (such as Austria, Canada, Italy, Spain, Türkiye, the UK and the U.S.), that support committee staff in budget analysis and contribute towards better transparency and parliamentary performance in budgeting.[19] However, in the defence and security field, the information publicly available has merely one source: the security agencies themselves. This monopoly of information compromises an objective, well-informed debate of budgetary issues. Parliaments make too little use of specialized independent bodies mandated to review and investigate the legality of public spending, such as supreme audit offices. Civil society organizations have only recently begun to focus on defence spending, and their research and analytical capacity is still developing.

Budget Execution

Budget execution refers to the continuous implementation of the budget law by government agencies. Once appropriations are approved, public entities are independent to spend funds, as long as they spend according to

[18] Ibid, p. 89.
[19] Ibid, p.92.

the approved objectives on a day-to-day basis. Ministries and government agencies have audit units responsible for internal control, whose organization and powers are defined by law in most countries.

There are several 'entry points' for parliamentary involvement and public debate during the budget execution phase. These include budget rectifications, parliamentary committee hearings and other oversight activities, and the debate of big procurement contracts.

All budget systems allow some modification of the budget during the execution stage through fund transfers, reprogramming, emergency bills and supplemental additions of new funding. Budget rectifications are proposed amendments to the main annual budget, submitted by the government to the parliament. They are often caused by unforeseeable activities such as newly mandated contributions to peacekeeping operations, natural disasters and other emergency situations. They are approved by parliament, following the same procedure as with other law proposals.

Parliaments oversee how the budget is spent through committee hearings, meetings with government representatives and visits to security sites and premises. Defence budget execution is one of the most important and frequent topics of oversight addressed by defence and security committees. Committees often issue press releases or even reports on the situation revealed during such oversight activities.[20]

Procurement contracts, through which national security authorities acquire goods and services, constitute a large portion of public expenditure. Due to their material impact on national industries, procurement contracts are susceptible to corruption; therefore, the integrity of defence and security procurement attracts increasing levels of public attention. A clear legislative framework to provide *inter alia* for a competitive procurement process is key for ensuring integrity. Single-source, or non-competitive procurement must be defined as an exception from the general rule, and the conditions should be clearly detailed in the law.

In some countries, important procurement contracts are subject to prior parliamentary scrutiny. This is notably the case in Germany, where contracts exceeding EUR 25 million must be submitted to the Budget Committee of the Bundestag for approval, and are extensively debated in the Defence Committee.[21] In the Netherlands, there is no fixed legal monetary threshold requiring parliamentary approval. However, for projects designated by Parliament as "major projects," political approval is in practice required, ensuring a high level of parliamentary oversight.[22] In other systems, even where formal approval is not required, governments are subject to strong transparency obligations. For example, in countries such as Hungary, Switzerland and the United Kingdom, the government must inform parliament or the relevant committee of significant procurement contracts and provide detailed information, enabling parliamentary scrutiny. In addition, some parliaments are involved upstream in the procurement cycle, including in defining capability needs, reviewing options, or assessing offset arrangements. This is the case, for instance, in Czechia and the United States.

Budget Evaluation

Budget evaluation is the expert examination of the compliance of an implemented budget with legal, financial and performance criteria. The relevance of this stage depends upon the way evaluation conclusions are undertaken by the government and incorporated in the next budget proposal. Effective criteria can help influence government decision-making, not only at the national level, but also at the international level, if malpractice and ineffectiveness are identified.

[20] For a review of committees' roles in budget oversight see Hironori Yamamoto, *Tools for Parliamentary Oversight: A Comparative Study of 88 National Parliaments* (Geneva: Inter-Parliamentary Union, 2007), pp. 19-22, http://archive.ipu.org/pdf/publications/oversight08-e.pdf.

[21] Germany. The Defence Committee tasks and procedures - The rights of the Defence Committee as regards preparation of the budget, https://www.bundestag.de/ausschuesse/verteidigung/arbeit-aufgaben-en-1096614 (accessed March 24, 2026).

[22] Netherlands. The Court of Audit, The Role Played by Parliament, https://english.rekenkamer.nl/topics/j/joint-strike-fighter/the-netherlands-as-a-purchaser-of-the-jsf/the-decision-making-process/the-role-played-by-parliament (accessed March 24, 2026).

Parliament, non-governmental organizations (NGOs), the media and the national Audit Institution may all play a role in this stage. They measure whether the public resources are spent efficiently and convey this information to the larger public.

The execution of the budget should end with the publication of annual activity reports and reports of budget execution (or report of accounts), which are the first sources of information on how money was spent by a government agency.

Since budget evaluations, and especially the financial component of audits, are expert endeavours, the National Audit Institution (sometimes called the Auditor General, National Audit Office, Budget Office or the Chamber of Accounts) plays a prominent role in this process. The institution is the state body which legally exercises the highest public auditing function of that state, conducting the detailed and professional financial audit of all government departments. The reports of the Audit Institution are presented to parliament and are made public. An example of efficient budget evaluation is the work of the UK's National Audit Office; its detailed scrutiny of departmental spending produced 61 reports in 2021.[23] It issues an annual Major Projects Report, which describes the largest defence procurement projects of the British MoD.[24]

Regardless of their power in other stages of the budget cycle, parliaments may play a decisive role in auditing defence expenditures through hearings, inquiries and public reports aimed at informing public opinion. These, in turn, can be heavily influenced by the research and lobbying of CSOs. If their recommendations shape budget formulation, this might diminish the need for amendments during the budget approval stage.

Ideally, audit reports issued by parliament and national audit institutions should enable the public to evaluate the legality, efficiency and effectiveness of government departments' spending.

Conclusion

Global military spending has reached the level of USD 2.7 trillion annually,[25] even before the start of the war in Ukraine which saw governments across Europe boost defence spending. Funding 'war and butter' will become an acute competition as the European peace dividend seems to be consumed, and limited resources must now respond to the new economic crises and threats to global security, such as climate change or cyberthreats, which are 'growing faster than our ability to prevent and manage them'.[26]

Parliaments can and should contribute to increased discipline, focus and integrity in public spending in defence and security through an improved understanding and effective participation in the state budgeting process.

Effective parliamentary participation in the state budgeting process is indispensable for the good governance of the security sector, ensuring that the budgeting process factors in the public's interests and preventing the misuse of public funds. Effective parliamentary participation in the state budgeting process ensures transparency in governmental decision-making about defence and security resources and keeps the public informed of significant developments which affect national security.

[23] National Audit Office (UK), *National Audit Office Publications*: https://www.nao.org.uk/search/sector/national-security/.
[24] National Audit Office (UK), *Improving the performance of major equipment contracts*, (London: National Audit Office, June 24, 2021), https://www.nao.org.uk/report/improving-the-performance-of-major-equipment-contracts/.
[25] Tian, Nan, Xiao Liang, Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida Karim, and Jade Guiberteau Ricard. *Trends in World Military Expenditure, 2024*. SIPRI Fact Sheet. Stockholm: Stockholm International Peace Research Institute, April 2025. https://www.sipri.org/publications/2025/sipri-fact-sheets/trends-world-military-expenditure-2024
[26] World Economic Forum*, The Global Risks Report 2022* (Geneva: World Economic Forum, January 2022), https://www.weforum.org/reports/global-risks-report-2022/digest.

13. Anti-Corruption Agencies

Francisco Cardona

Internationalization of Anti-Corruption Efforts

The recent global proliferation of anti-corruption agencies reflects growing concern about corruption as a major international problem. Corruption hinders economic development at the global level. The 2003 United Nations Convention against Corruption (UNCAC) and the 1999 Council of Europe Civil and Criminal Conventions have had a significant influence on the creation of Anti-Corruption Agencies (ACAs).

Corruption-related problems were traditionally considered a matter of domestic order. Discussing corruption and anti-corruption in another country was considered interference in the internal affairs of a sovereign country. The progressive internationalization of anti-corruption policies has represented, then, a remarkable change.

Little by little, international bodies such as the OECD, the World Bank, the Council of Europe, and the United Nations, among others, have noticed and acted upon corruption in all countries, both developed and less developed, and its effects on international trade. How and why was this international awareness raised? Law occupies a central role. Anti-corruption law is no longer only a national concern, but it is evolving into a global legal regime.[1]

One of the earliest efforts to combat international bribery was the United States' Foreign Corrupt Practices Act (FCPA), adopted in 1977. The law prohibits companies and individuals from bribing foreign officials to obtain or retain business, including through consultants, distributors, or joint-venture partners. Violations of the FCPA can result in significant administrative and criminal penalties, including the return of illicit profits, interest payments, and substantial fines. The law is enforced jointly by the U.S. Securities and Exchange Commission (SEC) and the Department of Justice.[2] The FCPA also laid the groundwork for international efforts to combat bribery. In 1997, the OECD Anti-Bribery Convention required major exporting countries to criminalize the bribery of foreign public officials in international business transactions. Before the Convention, the United States was the only country with such legislation. By 2024, the Convention had been signed or ratified by 46 countries.

The OECD Anti-Bribery Convention assures 'functional equivalence' among the measures taken by parties to sanction foreign bribery without requiring uniformity or changes in fundamental principles of a party's legal system. The work on the OECD Convention began in 1989. It aimed primarily to level the playing field for companies active on the international market. Companies originating from a country where bribery of foreign public officials was criminalized (essentially the United States) felt that they were facing competitive disadvantages for accessing international markets. Their counterparts included businessmen and women from countries where foreign bribery was tax deductible. The OECD work resulted in the development of the Recommendation on Combating Bribery in International Business Transactions, which was adopted at the ministerial level by the OECD Council in 1994. However, this was a 'soft law' solution, which was insufficient for addressing the problem of international corruption.

Debates were held on the best way to criminalize the bribery of foreign public officials in an effective and coordinated manner, as stated in the 1994 Recommendation. The different criminal law systems of the member countries turned reaching any agreement on the inclusion of identical provisions, either in a treaty or in implementing national legislation, into a significant challenge. To resolve these problems, the OECD developed the concept of 'functional equivalence.' Different approaches from signatory parties would be admitted,

[1] Régis Bismuth, Jan Dunin-Wasowicz, and Philip M. Nichols, *The Transnationalization of Anti-Corruption Law* (London: Routledge, 2021), https://doi.org/10.4324/9781003174639.

[2] For more details see Congressional Research Service, *The Foreign Corrupt Practices Act (FCPA): An Overview,* IF11588, In Focus, June 29, 2020, https://fas.org/sgp/crs/misc/IF11588.pdf.

provided they led to equivalent results, namely, effective prosecution and sanctions. The OECD focused on the supply-side of bribery, not on extortionary demands by foreign officials.

Based on the political commitment made by member states in the 1994 Recommendation and the work already accomplished since 1989, progress came rapidly. A negotiating conference of both the members and those non-members already participating in the preparations concluded negotiations on the text of the OECD Convention in November 1997.[3] The Convention was officially signed on 17 December, 1997 by all OECD members and five non-member countries.[4] The OECD Working Group on Bribery monitors countries' implementation and enforcement of the OECD Anti-Bribery Convention through a peer-review monitoring system. Parties to the Convention are subject to review by their peers, with experts from different countries at the Working Group on Bribery serving as assessors. Transparency International has identified this monitoring mechanism as the 'gold standard' of monitoring.

However, the very first multilateral anti-corruption convention that addressed both supply-side (active) and demand-side (passive or extortion) bribery was the Inter-American Convention Against Corruption (IACAC), adopted in 1996. Thirty-four nations of the Organization of American States (OAS) ratified the Convention. Unlike the OECD Anti-Bribery Convention (adopted in 1997), the IACAC was not primarily a U.S. initiative, nor was it modelled on the U.S. FCPA. The IACAC is generally viewed as a 'personal triumph' for then Venezuelan President Rafael Caldera.[5]

In 1999, the Council of Europe adopted the Criminal Law Convention against Corruption. Its implementation is monitored by GRECO (Group of States against Corruption) of the Council of Europe. The Civil Law Convention on Corruption was adopted in the same year, 1999.

While the IACAC was first and served as a model, the real globalization of the movement to address international corruption came through the 2003 United Nations Convention Against Corruption ('UNCAC'), which entered into force in 2005. It is signed or ratified by most UN member states (191 parties as of August 2025).[6] The UN Convention addresses five topics: prevention; criminalization and law enforcement measures; international cooperation; asset recovery; and technical assistance and information exchange. UNCAC addresses various forms of corruption, such as trading in influence and abuse of power, as well as various acts of corruption in the private sector. Within the prevention measures, it includes the creation of anti-corruption agencies (article 6) and anti-corruption specialized prosecutorial services or equivalents (article 36). The Implementation Review Group (IRG), the UNCAC's monitoring mechanism, was established in 2009 and has been operational since 2010. Still, there is no formal follow-up process on the findings and recommendations made in the implementation review cycles. Some countries report voluntarily to the IRG on actions they have taken after the completion of the review. Consequently, the UNCAC has a relatively weak implementation monitoring mechanism.

The internationalization of the anti-corruption movement is linked to the increasing globalization of the economy. Anti-corruption has come a long way since its first steps in the United States and, later, Venezuela. Difficult, protracted international negotiations have been necessary for the creation of an international level playing field against corruption, to contribute to the development of 'global governance.' Such standards are crucial in an area where national action alone is no longer able to adequately prevent corruption-associated risks. It is enough to think of: terrorism financing; organized international criminality; transnational money

[3] Mark Pieth, Lucinda L. Low, and Nicola Bonucci, eds., *The OECD Convention on Bribery: A Commentary*, 2nd ed. (Cambridge: Cambridge University Press, 2013).
[4] See Organisation for Economic Co-operation and Development (OECD), "Anti-corruption and integrity," OECD, n.d., https://www.oecd.org/gov/ethics/2406452.pdf.
[5] Elizabeth K. Spahn, "Implementing Global Anti-Bribery Norms: From the Foreign Corrupt Practices Act to the OECD Anti-Bribery Convention to The U.N. Convention Against Corruption," *Indiana International & Comparative Law Review* 23, no. 1 (2013), https://doi.org/10.18060/17871.
[6] "UNCAC Signature Elizabeth K. Spahn, "Implementing Global Anti-Bribery Norms: From the Foreign Corrupt Practices Act to the OECD Anti-Bribery Convention to The U.N. Convention Against Corruption," *Indiana International & Comparative Law Review* 23, no. 1 (2013), https://doi.org/10.18060/17871.
[6] United Nations Office on Drugs and Crime (UNODC), "UNCAC Signature and Ratification Status," https://www.unodc.org/unodc/en/corruption/ratification-status.html (accessed February 23, 2026).

laundering; unfair international trade; and the political role of multinational corporations by introducing the criminal liability of legal persons around the globe. For the last fifteen years, NATO has also launched initiatives to increase integrity and reduce corruption in the defence and security sectors of member nations and partners through its Building Integrity Programme.[7]

Anti-Corruption Agencies (ACAs)

In September 2015, the UN member states adopted the 2030 Agenda for Sustainable Development to guide national and global development efforts over the following 15 years. Corruption, poor governance, and illicit financial flows were all highlighted in the 2030 Agenda as threats to achieving those critical development aims. The 2030 Agenda has 17 Sustainable Development Goals and 169 targets, some of which are specifically designed for tackling corruption and ensuring more accountable institutions. Target 16.5 calls upon member states to consistently reduce corruption and bribery in all their forms. Target 16.6 urges member states to develop effective, accountable, and transparent institutions at all levels, and target 16.10 calls for member states to ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements, notably UNCAC articles 6 (corruption prevention) and 36 (criminal suppression of corruption).

The large number of bodies categorized as ACAs reflects the fact that the Convention and regional anti-corruption treaties and standards do not propose a single 'best' model for such bodies. The Convention focuses on function rather than form when prescribing how states can establish ACAs within national anti-corruption frameworks. This approach reflects the early 'functional equivalence' propounded by the OECD, which has proven to be a highly effective instrumental concept to establish anti-corruption mechanisms while pre-empting hollow institutional isomorphism across national borders.

An ACA may be defined as an independent institution, located at arm's length from executive government institutions, whose main function is to coordinate all activities geared towards the implementation of a country's anti-corruption strategy and to provide feedback for the redesign and improvement of that strategy. Investigation and prosecution may also form part of an ACA's functions. How the ACA is designed and located in the overall government structure is crucial both for preserving its professional autonomy and for institutional independence, and for ensuring its professional accountability and the evaluation of the agency over time. Design weaknesses, along with performance failures, will probably be conducive to an ACA's irrelevance.[8]

This definition is one among many, but the two major elements, functions (competences) and location (and therefore accountability lines), are the two variables that underlie the different definitions of ACA and various national models. As we will see, there are several ACA models in different countries depending on their functions, jurisdiction, and established accountability lines.[9]

Standards of ACAs

The standards for ACAs set up by international conventions, especially the UNCAC (articles 6 and 36) and the Council of Europe Criminal Law Convention on Corruption (article 20), are:

- Independence;
- specialization necessary for reliable expertise;
- adequate resources and staff size.

Independence has degrees. An ACA may enjoy a very high degree of independence or be awarded a lower degree, depending on the functions allocated to the agency. Independence means the ability to decide and act

[7] North Atlantic Treaty Organization (NATO), "Building Integrity," *What We Do, NATO*, last updated 22 January 2025, https://www.nato.int/cps/en/natohq/topics_68368.htm (accessed February 23, 2026).
[8] Francisco Cardona, "Anti-corruption Policies and Agencies," *Good Governance Guides* 3 (Oslo: Centre for Integrity in the Defence Sector, 2015), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/7/pdf/200724-BI-GGG3-en.pdf.
[9] Organisation for Economic Co-operation and Development (OECD), *Specialised Anti-corruption Institutions: Review of Models*, 2nd ed. (Paris: OECD Publishing, 2013), https://doi.org/10.1787/9789264187207-en.

impartially and without external influence, especially when it comes to investigative activities. This translates, *inter alia*, into protection from political interference and undue pressures of any kind. Independence is thus a value that cannot be achieved if the political will to fight corruption is weak or non-existent. If the main responsibility of the ACA is to educate, raise awareness, or fulfil a limited number of prevention responsibilities, the degree of independence required is relatively low. In such cases, independence beyond the general professional autonomy of the civil service is not essential. The same is true of policy analysis and policy recommendations. The more the functions lean in the direction of investigation and law enforcement, the more independence is required.

Specialization means that the law has established a focused, specific mandate for the agency and that the staff are professionally specialized. The staff must encompass all relevant skills needed for the ACA to fulfil its mandate or mission. Specialization is first and foremost required by the CoE Criminal Law Convention on Corruption (article 20) and the UNCAC (article 36) for law enforcement bodies such as anti-corruption prosecutors. In developed countries, specialization is often ensured by assigning anti-corruption tasks to existing persons or units within existing law enforcement bodies. In developing countries and countries in transition, where corruption is severe and the involvement of donors is more widespread, the trend has been to establish separate anti-corruption bodies to better guarantee specialization.

To achieve some success, specialized law enforcement anti-corruption bodies, especially anti-corruption prosecution offices, require at least the following capacities. First, they must specialize in and focus on serious criminality by leaving petty corruption to the regular prosecution offices. Second, ACAs should work in close cooperation with a police unit highly specialized in complex economic and financial criminality and have access to relevant expertise of different types, in particular, auditors and other professionals from ministries of finance or audit institutions, as well as IT specialists. Third, judges need to have an equivalent degree of specialization to that of prosecutors. Fourth, the jurisdiction of the ACA, as well as that of specialized judges, needs to be national and cover the whole territory without restrictions. Fifth, the description of criminal corruption-related actions in the penal code must be clear and unambiguous, and the legislation on criminal proceedings must be coherent. Sixth, the lines of accountability of specialized anti-corruption prosecutors, from the bottom up to the general prosecutor, need to be clear and effective in practice. The professional independence of prosecutors must also be sufficiently protected by legislation. Finally, investigative capacities and effective means of gathering evidence are indispensable. We refer, *inter alia*, to undercover investigations; wiretapping; access to bank accounts; and sound witness and whistleblowing protection measures.

Factors for Success and Failure of ACAs

The sustainability of ACAs is never guaranteed. Many countries face serious difficulties in meeting international standards for political or other reasons. Corruption prevention and control are highly competence-based governmental and non-governmental policy processes aimed at curbing the incidence and scope of corruption. Those processes require a combination of guiding principles and instruments. Efforts to make corruption control more effective require a complex mix of repressive and preventive approaches, of incentives and restraints, of internally and externally imposed standards of integrity, of procedural, institutional, structural, and educational measures, of interrelated control mechanisms, as well as of enforceable laws, ethical principles, and moral guidance. However, overstated expectations of an ACA without introducing reforms to improve the general governance of a country, not least the political processes, are misplaced and may be counterproductive, as the case of Portugal shows in the box below.

Box 13.1. Closing Down an ACA for Political Reasons: The Case of Portugal

The case of the Portuguese ACA (*Alta Autoridade Contra a Corrupção*) is illustrative. The demise of the Portuguese ACA was not related to its objective performance, which was reputed to be good, but to the tensions between the agency and the political class. The agency's work often challenged the interests of politicians. The Portuguese agency was perhaps the first ACA to appear in the Western world. It was established in 1983 by government decree as part of a political thrust to minimize public discontent with patronage-ridden party politics. It was not supposed to investigate corruption in political parties. In 1986, it was given investigative powers and started to make inroads into and threaten the interests of the political establishment. It was terminated, without any debate on its performance, by an act of parliament in 1992, just when other Western countries were thinking of creating anti-corruption agencies.[10] Of note, Portugal established the National Anti-Corruption Mechanism under Decree-Law No. 109-E/2021 of 9 December 2021 as part of the country's National Anti-Corruption Strategy. The mechanism gradually became operational between 2022 and 2023, following the appointment of its leadership and the adoption of implementing regulations enabling the institution to begin its activities.[11]

Johnsøn et al. systematized the extant literature on success factors into five factors:[12]

1. *Contextual factors*: The degree of success of ACAs must be seen in context. Organizational cultures, levels of national development, and political stability set the backdrop for these bodies. It can hardly be expected that an ACA will function adequately in a country with serious governance problems.
2. *Legal framework and policy factors*: ACAs encounter various constraints on their mandate because of policy choices during the legislative process. These may determine: their legal status; institutional location; special powers; sharing of competences and information; financial autonomy; reporting procedures, etc. Under their statutes, all ACAs are in some sense independent. In practice, however, the degree of operational autonomy varies considerably from one agency to another. ACAs also often lack the authority to ensure that other public institutions enforce their recommendations. In many cases, ACAs are operationally and financially independent in name only. In most cases, the legal framework for inter-institutional collaboration is not properly addressed at the outset. In addition, ACAs often find themselves stretched to deliver on overly broad mandates. Multipurpose agencies are often expected to clamp down on corruption (a fear-based function), while at the same time serving as an advisory body on prevention (a trust-based function).
3. *Organizational factors*: Low levels of performance also derive from inadequate recruitment and accountability procedures, as well as inadequate or non-existent management arrangements that determine an organization's capacity to operate and deliver on its mandate. The technical capacity of an ACA can also be hampered by ineffective collaboration with other authorities. Difficulties in obtaining evidence about corruption practices or information about risk areas from other state bodies or agencies reduce the effectiveness of ACAs.
4. *Financial factors*: Lack of sufficient financial resources is a constant threat to any organization. While large budgets do not necessarily generate greater levels of productivity, it is important to note that

[10] Luís de Sousa, "Does Performance Matter to Institutional Survival? The Method and Politics of Performance Measurement for Anti-corruption Agencies," *EUI Working Paper RSCAS* 2009/9 (European University Institute, 2009), http://hdl.handle.net/1814/10689.

[11] Council of Europe, Group of States against Corruption (GRECO), *Fifth Evaluation Round: Preventing Corruption and Promoting Integrity in Central Governments (Top Executive Functions) and Law Enforcement Agencies—Compliance Report: Portugal*, GrecoRC5(2025)7 (Strasbourg: Council of Europe, March 19, 2025).

[12] Jesper Johnsøn, Hannes Hechler, Luís de Sousa, and Harald Mathisen, "How to Monitor and Evaluate Anticorruption Agencies: Guidelines for Agencies, Donors, and Evaluators," *U4 Issue* no. 8 (Chr. Michelsen Institute, 2011), http://www.cmi.no/publications/file/4171-how-to-monitor-and-evaluate-anti-corruption.pdf.

some ACAs work under strained financial conditions that may seriously compromise their effectiveness in pursuing set objectives.

5. *Leadership and expertise factors*: The individual skills, experience, and knowledge of ACA staff are fundamental to their success. Capacity issues concern both the technical capacities of ACAs and their overall functional capacities (such as leadership, human resource management, planning, and organizational learning). One of the advantages of ACAs in comparison to traditional law enforcers is their capacity to generate a knowledge-based approach to the fight against corruption through risk assessments and other specialized studies. In principle, these bodies should be equipped with a team of experts who can also draw on the knowledge and experience of other monitoring and regulatory units, and share their own expertise in exchange. In practice, however, very few ACAs have access to in-house research and similar knowledge-production capacities.

To these five factors, two additional ones may be added:

6. An extended set of success factors includes ACAs cooperating with anti-corruption stakeholders both domestically and internationally, such as the media, major NGOs, universities, and other ACAs around the world. This kind of cooperation is useful for gathering information, developing knowledge, obtaining technical and political support, and creating synergies concerning specific corruption investigations domestically and across borders. Disseminating 'good practice' through international and domestic networking may represent a strong endorsement of the role and position of an ACA.
7. Adequate accountability mechanisms help ensure the legitimacy and credibility of an ACA, and therefore, increase its likelihood of success. Indeed, however autonomous and independent an ACA might be on paper, it has to be integrated into the checks-and-balances system of a given country. As noted earlier, independence has degrees. International standards on ACAs, especially the UNCAC and the CoE Convention on Criminal Law, do not demand the same degree of independence as required by judges. According to the OECD, the forms of accountability have to be tailored to the ACA's level of specialization, institutional placement, mandate, functions, and powers *vis-à-vis* other institutions and individuals.[13]

In 2020, the United Nations identified the factors of success of anti-corruption agencies in similar terms.[14]

Suppression and/or Prevention of Corruption?

Anti-corruption efforts vary across countries, cultures, and different models. Some emphasize the suppression of acts of corruption; some the prevention of corruption and the promotion of integrity. Both approaches are necessary and should be adopted simultaneously. In the 2013 OECD classification cited above, there is a rather clear-cut division between law-enforcement approaches and prevention approaches. This classification clearly distinguishes between national policy choices.

Countries that rely almost exclusively on the penal code and the criminal justice system to deal with corruption tend to have more perceived corruption than countries that devote significant resources and efforts to corruption prevention policies. However, the penal code, albeit indispensable, is insufficient and has insurmountable limitations in the fight against corruption. In the Western tradition, the presumption of innocence, fortunately, is a fundamental tenet of criminal law, and in many countries this principle has been given constitutional status. Nobody can be convicted of a crime unless he or she is proven guilty beyond a reasonable doubt, as judged from the evidence presented by the prosecutor. This evidence must be clear and convincing. But acts of corruption tend to be extremely difficult to prove. Corruption is a concealed, clandestine activity. Those who are enmeshed in corrupt behaviour tend, after all, to disguise their illicit activities. No criminal judge with professional integrity will convict a politician, public official, or corporate tycoon without clear and

[13] Organisation for Economic Co-operation and Development (OECD), *Specialised Anti-Corruption Institutions: Review of Models: Second Edition*, (Paris: OECD Publishing, 2013) https://doi.org/10.1787/9789264187207-en.
[14] *Colombo Commentary on the Jakarta Statement on Principles for Anti-Corruption Agencies* (Vienna: United Nations Office on Drugs and Crime, 2020), https://www.unodc.org/documents/corruption/Publications/2020/20-00107_Colombo_Commentary_Ebook.pdf.

convincing evidence. This represents a major, but necessary, limitation of the penal code in the effort to fight corruption. In addition, the penal code must be clear in defining criminally punishable offences. Vague wording in the legal description of illicit behaviour in the penal code may often lead a judge to acquit a suspect.[15]

Prevention by way of fostering and protecting public integrity, therefore, is indispensable. Democratic political regimes and countries with strong preventive policies in place from robust governance systems are perceived as being less corrupt than authoritarian countries without such policies in place. Preventive policies require an administrative and public law framework capable of reducing vulnerabilities to corruption in public bodies in a proactive way, while preserving values like the efficiency and effectiveness of well-functioning public administrations. This is the policy followed by countries such as Australia, the United States, New Zealand, Germany, and, especially, the Scandinavian countries. They have endeavoured for years, some of them for centuries, to promote transparency in public administration, with strong checks and balances, accountable administrators, and professional, patronage-free civil services. These are the most robust pillars of preventive anti-corruption policies.

Combating Corruption in the Defence and Security Sectors

Both articles 6 and 36 of the United Nations Convention against Corruption explicitly call for the 'necessary independence' of ACAs. Particularly for ACAs with a mandate to investigate and/or prosecute or judge corruption cases, it is essential that the ACA is, and is seen to be, impartial and neutral. Specialized anti-corruption prosecutors and anti-corruption courts fall entirely within this requirement of independence and impartiality. Impartiality means that the ACA must not be seen as biased for or against any stakeholders, for example, it should not be based on race, gender, religion, class, or group loyalty. Neutrality requires that the ACA can be trusted not to take sides in cases except as required in defence of the law. A similar requirement can be found in article 20 of the Council of Europe Criminal Law Convention against Corruption.

The traditional secrecy and exclusiveness of the security and military domains have tended to constrain transparency, accountability, and independent oversight in these sectors. The need for confidentiality in some areas of the defence sector is often overused and reduces opportunities for scrutiny by oversight bodies in government, the judiciary, and civil society. Official secrecy, justified on grounds of national security, is too often used to avoid political embarrassment or to cover up corruption.[16]

Most countries, however, do not have anti-corruption agencies specialized in defence and security matters. Nevertheless, as a rule, the mandate of national ACAs covers all public organizations, including the military and, in some cases, private organizations.[17] Importantly, they have the mechanisms needed to circumvent the challenges of secrecy and exclusiveness and have made a visible impact on the defence sector. Box 13.2 below provides a number of examples from around the world. In all cases including arrests, officials detained by ACA are considered innocent until a court decides otherwise.

[15] See for example, Dylan Tokar, "Dispute Over Agency in Foreign Bribery Case Gets Second Hearing," *Wall Street Journal*, August 17, 2021, https://www-wsj-com.cdn.ampproject.org/c/s/www.wsj.com/amp/articles/dispute-over-agency-in-foreign-bribery-case-gets-second-hearing-11629240990 (accessed February 23, 2026).
[16] Francisco Cardona, *Balancing Openness and Confidentiality in the Defence Sector: Lessons from International Good Practice* (Oslo: Centre for Integrity in the Defence Sector, 2018), https://cids.no/wp-content/uploads/2018/06/9062-DSS-GGG-6-eng-4k.pdf.
[17] See, for example, the mandate of the ACA of France: "About Us," l'Agence française anticorruption (AFA), n.d., https://www.agence-francaise-anticorruption.gouv.fr/en/lagence (accessed February 23, 2026).

Box 13.2. Examples of ACAs' Activities in the Defence and Security Sector

[Author: Prof. Todor Tagarev]

Raising Awareness. Officials from the Anti-Corruption Commission of Sierra Leone organized a series of events in early 2024 with senior personnel from the country's system of military hospitals. The meetings focused on the comprehensive negative impact of corruption and underlined the importance of prevention, moral values and codes of ethics, while strengthening institutional strategies.[18]

Investigative powers. In 2023, the Anti-Corruption Committee of the Republic of Armenia carried out large-scale operative-investigative measures. These led to the arrest of military officers, including the commander of a logistics unit, for demanding and partially receiving a bribe of AMD 19.5 million (approximately EUR 50,000) from the director of a garment factory. In return, the commander agreed to accept the delivery of garments not meeting the technical specifications and required sizes. Further, the investigation, conducted jointly with the Military Police, revealed earlier cases of bribes given by the same company and the delivery of substandard products.[19]

Seizure of Assets. In 2025, the Anti-Corruption Commission of Bangladesh has launched an investigation into alleged corruption, illegal wealth accumulation, and money laundering involving, among others, at least ten former senior military officials, including a former army chief and heads of intelligence agencies. According to public reports, some of the investigations have already led to formal cases, asset seizures, and travel bans.[20]

Cooperation with Military Prosecutors. In July 2025, officers of the Polish Central Anti-Corruption Bureau (CBA) detained four men on the order of a military prosecutor. CBA officers searched several locations in four cities in Poland and found evidence of collusion to unlawfully influence the results of tender procedures conducted by military units.[21]

Investigations in the internal security sector. In 2025, the National Anti-Corruption Commission of Australia published reports of suspected nepotism and cronyism. In Operation Kingscliff, an investigation was conducted into whether a senior executive officer from the Department of Home Affairs had improperly used her position to influence employment processes to the benefit of her sister and her sister's fiancé. The investigation concluded that the official had abused her public office and misused official information: corrupt conduct that was both serious and systemic. The Commission also came up with a set of recommendations to the Department to strengthen policies and reduce corruption risks in recruitment.[22] In Operation Wilson, the Commission investigated a joint report by the Australian Federal Police and Victoria Police on the involvement of a border police officer in illicit imports of tobacco. The investigation resulted in a guilty plea and two charges.[23]

[18] Yangie D. Sesay, "ACC Engages 34 Military Hospital on Corruption Risks in Service Delivery," Anti-Corruption Commission of Sierra Leone, February 2024, https://anticorruption.gov.sl/blog/anti-corruption-commission-sl-news-room-1/post/acc-engages-34-military-hospital-on-corruption-risks-in-service-delivery-1237.

[19] "The commander of the military unit of the military base of the Ministry of Defense is taken into custody on the charge of accepting bribe of more than 19 million AMD; persons who paid bribes and assisted in accepting bribes were also taken into custody," Anti-Corruption Committee of the Republic of Armenia, July 14, 2023, https://www.anticorruption.am/en/post/the-commander-of-the-military-unit-of-the-military-base-of-the-ministry-of-defense-is-taken-into-custody-on-the-charge-of-accepting-bribe-of-more-than-19-million-amd-persons-who-paid-bribes-and-assisted-in-accepting-bribes-were-also-taken-into-custody.

[20] Jasmin Moli, "Bangladesh's Anti-Corruption Dragnet Hooks 10 Former Top Military Generals," *bdnews24.com*, June 8, 2025, https://bdnews24.com/bangladesh/5cd4143aa215 (accessed February 23, 2026).

[21] CBA Press Team, "Corruption Scheme in Public Tenders," News, Central Anti-Corruption Bureau (CBA), July 2025, https://www.cba.gov.pl/en/news/1379,Corruption-Scheme-in-Public-Tenders.html (accessed February 23, 2026).

[22] "Case Study - Operation Kingscliff," National Anti-Corruption Commission, June 2025, https://www.nacc.gov.au/case-study-operation-kingscliff (accessed February 23, 2026).

[23] National Anti-Corruption Commission, *Investigation Report - Operation Wilson*, (Canberra: National Anti-Corruption Commission, 2025), https://www.nacc.gov.au/sites/default/files/documents/2025-02/Operation%20Wilson%20-%20Investigation%20Report.pdf.

Conclusion: Lessons from Institutionalizing Anti-corruption Policies and Agencies[24]

Diagnosis is an essential first step in treating corruption. Corruption is such a complex phenomenon that pursuing simplistic approaches can do more harm than good. Corruption will only be reduced by steadily and resolutely upgrading all the essential elements of the integrity system, both in political and administrative sectors and in public and private sectors. To achieve this, both preventive and repressive measures are needed. Building a robust integrity system represents a major political and technical effort that needs to be sustained over time.

Combating corruption is a multi-faceted endeavour. All major international treaties recognize the multidimensionality of the phenomenon. The 2003 UNCAC is a good example of the diversity of aspects and fields that need to be addressed to make any anti-corruption effort both credible and workable. The same complexity is observable in the two conventions – criminal and civil – of the Council of Europe against corruption. A single institution concentrating all or most powers is unlikely to cope effectively with all aspects that need to be addressed.

Concentrating all anti-corruption efforts within a single institution (especially if it is new) could jeopardize the anti-corruption drive and facilitate the illicit capture of the anti-corruption struggle itself. A plurality of institutions acting in several fields (parliament, government, judiciary, public administration, and local governments) may contribute better to the anti-corruption effort as a whole, provided that they are adequately institutionalized, resourced, and networked.

Around the world, integrity has become a critical consideration for administrators when filling civil service positions and for voters when comparing candidates for elected or political office. Integrity is now promoted through a broad variety of means. This includes: the introduction of leadership codes of conduct; declarations of personal assets; monitoring personal assets; training and education; transparency in public administration and politics; and personal accountability.

The realization that institutions are interrelated and that reforms must often be coordinated has also led to an expansion of the notion of 'separate' institutions and of the list of institutions commonly included in anticorruption strategies. Much of the focus remains on key elements of public administration, including financial control agencies, the court system, prosecutorial law enforcement and other criminal justice agencies, as well as bodies that deal with public service staffing and the procurement of goods and services. However, it is now understood that other institutions of government and civil society require attention as well. Only then will a systemic approach to combatting corruption be truly systemic.

Key public sector groups that should be included in such systemic strategies are: parliaments, governments, and public administrations at the national, regional, and local levels; the judiciary and its supporting institutions; key watchdog agencies, such as auditors or inspectors; and law enforcement agencies and other elements of criminal justice systems. Any credible strategy ought to always cover local self-governments and financing of political parties and electoral campaigns.

International experience shows that centralized watchdog agencies have achieved some success only in countries where governance is generally good. In most OECD countries the anticorruption effort and implementation of pro-integrity policies are not monopolized by a single agency or institution. A plurality of institutions and mechanisms are in place, each with different responsibilities and roles, and usually with the capacity to check on each other while, at the same time, networking. In weak governance environments, anti-corruption agencies have been created, often upon external pressure. But they frequently lack credibility and may even extort benefits for themselves. Often, they are captured by vested interests, either licit or illicit, or both. In general, they prove to be ineffective.

[24] Based on Francisco Cardona, "Anti-corruption Policies and Agencies," *Good Governance Guides* 3 (Oslo: Centre for Integrity in the Defence Sector, 2015), https://www.nato.int/nato_static_fl2014/assets/pdf/2020/7/pdf/200724-BI-GGG3-en.pdf.

Poorly embedded anti-corruption bodies in the broader political and administrative institutional landscape tend to be another major and more universal cause of failure. The chief lesson to be drawn from such failures is that the priority should be given to concentrating on reform efforts that strengthen all the various democratic governance systems in a given country. Without this groundwork on the key governance components, any specialized institution is likely to fail.

Political will shapes the role of the government in preventing and fighting corruption, particularly in the case of a democratically elected president or cabinet of ministers with a determined political will. Moreover, political will is crucial for the effective enforcement and review of existing legislation, and for proposing amendments to fill gaps and loopholes. Political commitment is vital to reforming those governance systems so as to make them function effectively.

International cooperation is valuable provided that international organizations or bilateral cooperation do not impose any specific institutional or organizational solutions. Policy dialogue should concentrate principally on the governance principles to be promoted and guaranteed, and the outcomes to be produced, rather than on the ways and means to achieve them. This is crucial in preventing the cultural rejection of foreign-imposed models. All too often these are presented as having universal application, though they grew out of specific historical and political circumstances. Local context is vital, and local ownership paramount. Principles and standards, however, are universal.

14.Civil Society and Defence Institutions

Dr. Stephanie Trapnell, Matthew Steadman, and Dr. Michael Ofori-Mensah[1]

Introduction

Historically, the role of civil society actors in the formulation of defence policy and defence decision-making has been minimal.[2] But defence governance pertains to much more than military manoeuvres and the state of the armed forces. It is about how authority is exercised in the management of defence institutions and policies. Even though defence and security issues are often held up as exceptional and outside the remit of standard governance reform, the principles of good governance still apply. Citizens should expect capable, efficient, open, inclusive, and accountable institutions that manage defence policies and practice.

Governance failures within the defence sector often reflect larger, systemic issues with democratic institutions of accountability, as well as with transparency mechanisms throughout government. This translates into vulnerabilities within core defence functions that increase corruption risks. Along with key institutions such as parliament, the judiciary, and the executive, civil society actors play a critical role in not only mitigating corruption risk, but also ensuring good governance and democratic oversight.

This chapter discusses the importance of transparency and civic space to defence governance, as well as presenting a case for the inclusion of civil society actors in its policy, planning, and implementation. It begins with a brief review of the democratic foundations of defence governance, and then discusses the variety of roles that civil society organizations can play within and outside defence governance institutions. The next section introduces the Government Defence Integrity Index (GDI), which presents a typology of corruption and integrity risks that are specific to the defence establishment. Using GDI 2020 data, this chapter presents findings for NATO countries regarding defence transparency and civic space, highlighting areas of strength and vulnerability across member states, and discussing how these elements translate into effective defence governance.

Democratic Control of the Armed Forces

Civilian control of the armed forces is constituted by a hierarchical relationship between civilians and the military. Civilian representatives in Parliament make decisions that are binding for society as a whole, while the military is responsible for advising on and implementing any decisions that have been delegated to them by civilian decision-makers. In terms of civilian control, *civilians* are considered those members of the executive, the judiciary, and legislative branches of national government that decide on the 'authoritative allocation of values for a society'[3] and formulate, implement, and oversee the implementation of these political and governance decisions.[4] The degree of civilian control depends on the authority accorded to civilian decision-makers to make socially binding decisions, as well as civilian oversight in ensuring that the military fulfils its delegated functions in the way that civilians want.[5]

The institutions of **authority** define the extent of civilians' autonomous decision-making power over policies. These institutions include formal rules that ensure civilians' right to propose and enact legislation in all political matters, such as internal security, defence, and military policy. This also runs to decisions on matters of war and peace and domestic emergency situations. They also include effective organizations such as defence ministries

1 The chapter was written for Transparency International, Defence & Security.
2 What is meant here is the exclusion of civil society actors from the process of decision-making and policy-making, a process which might include consultations, forums, and other institutionalized means of discussion and decision-making that occur directly with defence actors, rather than occurring outside defence institutions.
3 David Easton, *A Systems Analysis of Political Life* (New York: John Wiley & Sons, 1967), p. 3.
4 David Kuehn, "Institutionalising Civilian Control of the Military in New Democracies: Theory and Evidence from South Korea," *GIGA Working Papers* no. 282, February 2016, p. 6, https://www.giga-hamburg.de/assets/pure/21197840/wp282_kuehn.pdf.
5 Ibid, p. 6-7.

and legislative committees with actual decision-making power and with civilians in command, absent undue influence from active or retired military personnel.[6]

Oversight institutions enable civilians to monitor and direct the implementation of decisions delegated to the military, and to punish military misbehaviour. These institutions have regulations on ministerial oversight, legislative scrutiny, and defence policy, military policy, and budgets, as well as on the judicial accountability of the military. In addition, these institutions have legislative committees, auditing chambers, and courts that are mandated and able to oversee and direct the military's operations and to punish military 'shirking.'[7]

While civilian control of the armed forces is a critical element in maintaining centralized and cohesive military institutions, it is insufficient on its own. Authoritarian regimes exert considerable civilian control over the military, but such forms of oversight are incompatible with democracy.[8] In addition to civilian control of the armed forces, democratic models are defined by the principles of good security governance, while also ensuring effective governance. Democratic control of the armed forces is constituted by four key elements:[9]

1. Legally defined institutional responsibilities and relationships that place the armed forces under clear civilian control;
2. The depoliticization of armed forces and the removal of their influence from domestic politics, particularly in post-conflict and transitional settings;
3. Mechanisms for the effective, transparent, and accountable implementation of defence policy and the defence budget;
4. The wider engagement of civil society in defence matters.

Civil society in this instance can be widely defined, depending on the circumstances. But it always includes domestic civil society organizations that are independent of the government in both policy and practice, as well as citizens who can safely weigh in on matters of national security. Additionally, it may include international non-governmental organizations (NGOs) that work at the global level, and in partnership with national organizations.

Roles of Civil Society

Civil society actors play a variety of roles *vis-à-vis* government entities. For example, civil society can play a key role in the development of policy by lobbying for changes and by contributing to citizen oversight of the government's work and mandate. Among other activities, this can include monitoring how public services, such as defence and security, are delivered, and how human rights are both violated and upheld by government actors.[10] In relation to the defence sector, civic space and civil society engagement are crucial for strengthening the defence governance chain; from lobbying and communicating public opinions during policy formulation; and in supporting and monitoring the implementation of reforms and service delivery.[11] Often, civil society organizations (CSOs) play more than one role at a time:

Advocacy: Traditionally, the role envisioned for civil society actors is in an initiating role. This is the role most often identified as 'advocacy,' in which a cause is identified, and other actors are persuaded to commit to a collective action process, such as a campaign or a protest. But advocacy also involves public education, awareness-raising, and coalition-building in domestic and international spheres of activity. Civil society actors work not only to bring societal issues and challenges to the attention of a wider public, but also to promote

[6] Aurel Croissant and David Kuehn, *Militär und zivile Politik (Military and Civilian Politics)* (Munich: Oldenbourg, 2011).
[7] Peter D. Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, MA: Harvard University Press, 2006).
[8] Hans Born, "The Role of Parliaments," in *Oversight and Guidance: Parliaments and Security Sector Governance*, edited by Eden Cole, Philipp Fluri, and Simon Lunn (Geneva: DCAF and NATO Parliamentary Assembly, 2015), p. 68, https://www.dcaf.ch/sites/default/files/publications/documents/Oversight%20and%20Guidance%20Parliaments%20and%20SSG_eng.pdf.
[9] Timothy Edmunds, *Defence Reform in Croatia and Serbia-Montenegro* (London: Routledge, 2003).
[10] Augustin Loada and Ornella Moderan, *Civil Society Involvement in Security Sector Reform and Governance*, Tool 6 (Geneva: DCAF – Geneva Centre for Security Sector Governance, 2015), p. 3, https://www.dcaf.ch/sites/default/files/publications/documents/ECOWAS_Toolkit_T6_EN.pdf.
[11] Ibid, 22.

fundamental and universal values.[12] They can serve as 'thought leaders' that advocate for important changes in the way that services are provided and the content of public policies. In the last ten years, there has been a proliferation of partnerships and cooperative ventures between international NGOs based in donor countries and CSOs based in the Global South, which focus on issues affecting their own communities or nations. This has allowed civil society actors to create space for new norms and standards that shape governance and state activity, for example in the Arms Trade Treaty.

Facilitation: Civil society actors also serve as catalysts and intermediaries, which is especially true of well-connected and well-established organizations that have gained the respect of a wide range of parties. Facilitation can include capacity building that contributes to citizen engagement and increased knowledge of rights and responsibilities. It also involves the establishment of dialogues among a range of actors, and particularly, by giving power to the voice of the marginalized and under-represented in formal venues.

Expertise: Civil society actors often have as much, or more, knowledge about a field of activity as government or military actors. This is particularly true for CSOs that work directly with communities, allowing for deep knowledge of local conditions and community needs. But it is also the case for international NGOs, which can provide a global, comparative view of the field, and can produce frontier research and analysis. When combined, CSOs at either level (domestic or international) can serve as translators of knowledge, e.g. domestic CSOs have an understanding of what matters for their constituents and context, while international NGOs often have a strong grasp of global-governance structures and funding mechanisms.[13] This knowledge translates into a pool of expertise that can add tremendous value to policymaking and service delivery, including policing, border security, and military operations.

Consultation: CSOs with varying kinds of expertise and knowledge are important for consultative processes. They can offer practical, tangible inputs into policymaking processes. They can identify areas in need of attention, and critical factors in the success of government ventures. As with facilitation, civil society actors in consultative processes can amplify the voices of the marginalized, who may be the most affected by policy changes or new initiatives.

Monitoring: 'Watchdog' is a common description of civil society actors in the field of integrity. Civil society actors are expected to hold institutions to account and promote transparency and accountability while doing so. This characterization obscures the critical element in monitoring government actions: transparency. CSOs need access to information about government activities as well as its decision-making processes. Without this knowledge CSOs are not able to properly, and appropriately, monitor whether the actions taken by the government or security providers are meeting targets and producing successful outcomes.[14] The role of civil society as a monitor, while often considered to be antagonistic, can in practice be complementary and extremely productive. Both government and communities benefit when services are delivered well. Cooperation around monitoring activities can improve efficiency in the use of resources, improve effectiveness, increase trust, and ultimately serve as a mutually beneficial foundation for further collaboration.

Implementation: Civil society actors can also work with, or for, government actors to provide services to communities, particularly at the sub-national level. However, in the defence and security sector, it is more difficult to envision a role for civil society as implementing actor unless the scope of action is widened beyond that of providing security. For example, CSOs may be able to implement disaster management, preparedness

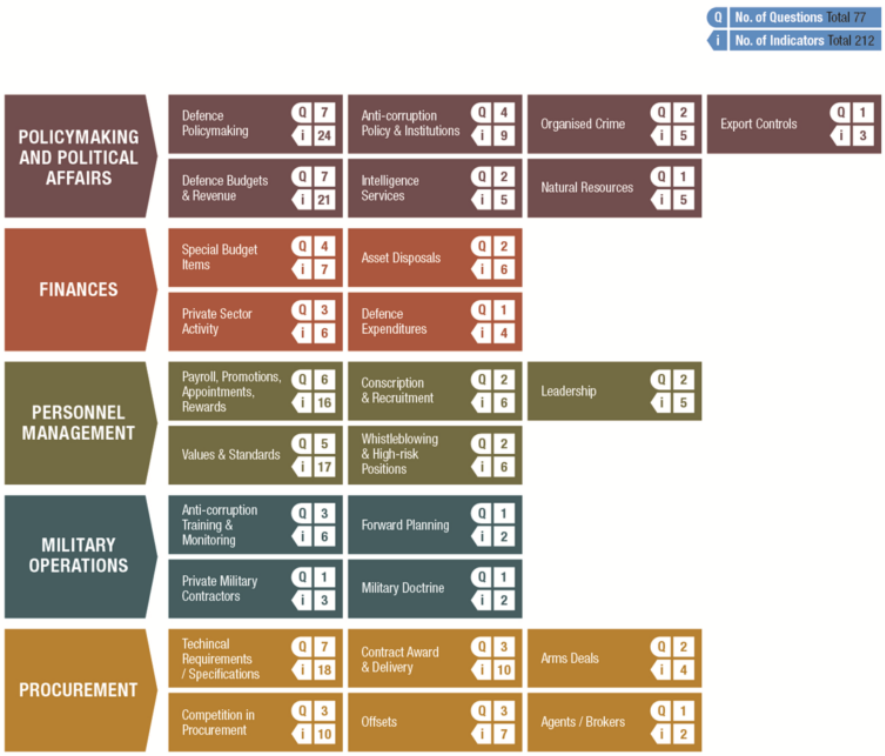
[12] World Economic Forum*, The Future Role of Civil Society* (Geneva: World Economic Forum, 2013), https://www3.weforum.org/docs/WEF_FutureRoleCivilSociety_Report_2013.pdf.
[13] These areas of expertise can also overlap greatly between international NGOs and domestic CSOs.
[14] Access to information includes (1) the regular, proactive disclosure of information and (2) the release of information in response to specific requests. For government actors, the responsibility of administering access to information involves not only disclosure, but also clarification and dissemination of information to stakeholders, as well as a commitment to information integrity. For additional discussion, see recent publications by Transparency International, Defence & Security: *Unlocking Access: Balancing National Security and Transparency in Defence (2024)* and *Creating Access: Strengthening and Expanding Information Governance in Defence (2025).*

and emergency response more effectively than government entities because of their embeddedness in communities and deep local knowledge. More than any other role outlined above, implementation is the most varied of the roles of civil society, as it may involve training, awareness-raising, facilitation, monitoring, and actual provision of services. CSOs may also play a substantial role in resilience enhancement initiatives that support MoD preparedness and response strategies. Any role in which civil society assists or substitutes government actors can be considered implementation, and it is one of the most cost-effective uses of government resources, particularly when budgets are stretched thin and/or acquiring staff expertise or gaining access to communities is cost prohibitive.

Civil Society Engagement in the Defence Sector: Government Defence Integrity Index

Transparency and civic space are deeply intertwined in the governance of public-sector functions. They are mutually reinforcing elements of democratic oversight. Without transparency, civil society faces obstacles in carrying out their roles, and in turn, the civic space of defence is bolstered by transparency, providing the enabling environment for civil society to thrive, and to support democratic processes and integrity building.

The Government Defence Integrity Index (GDI) is the only tool available for assessing the state of transparency and civic space in the defence sector.[15] The GDI presents a typology of corruption and integrity risks that are specific to the defence establishment. These risks form the basis for an assessment of the strength of institutional safeguards against corruption in defence sectors around the world, and capture the functioning of governance mechanisms across government. The index includes a number of indicators on transparency and civic space that aim to measure the commitment of governments to transparency and accountability, as well as their openness to civil society engagement. The index consists of five main risk areas: *policymaking and political affairs; finances; personnel management; military operations; and procurement.*



Source: Transparency International Defence & Security, *Government Defence Integrity Index (GDI): Methodology and Indicators* (London: Transparency International UK, 2020), https://ti-defence.org/gdi/methodology/the-gdi-indicators/

[15] Transparency International Defence & Security, *Government Defence Integrity Index*, n.d., https://ti-defence.org/gdi/ (accessed February 23, 2026).

Indicators allow the GDI to drill down in fine detail on a variety of issues across the broad field of defence sector governance. In order to provide a broad and comprehensive reflection of these risk areas, the index assesses both legal frameworks and implementation, as well as resources and outcomes. This is intended to capture the implementation gap between law and practice, and target areas to encourage reform to narrow this gap.

The scoring rubric has five levels of scores from 0–100, with the highest score indicating the most robust institutional resilience to corruption for the area:

Range of Scores					Corruption Risk
A	83	-	100	*Very robust institutional resilience to corruption*	Very low
B	67	-	82	*Robust institutional resilience to corruption*	Low
C	50	-	66	*Modest institutional resilience to corruption*	Moderate
D	33	-	49	*Weak institutional resilience to corruption*	High
E	17	-	32	*Very weak institutional resilience to corruption*	Very high
F	0	-	16	*Limited to no institutional resilience to corruption*	Critical

The resulting data is relevant for understanding the power politics that are at play in any defence policymaking process, as well as the institutional arrangements that structure how well the sector is managed. This provides both a gauge of corruption vulnerabilities, as well as a snapshot of the quality of governance across parliaments, the military, and the public sector, with a specific focus on independence and undue influence, transparency, oversight, and civic space. The GDI can be used for a variety of purposes:

- Identification of strengths and weaknesses in government defence integrity for individual countries;
- Score benchmarking with other countries and other datasets;
- Policy solutions using contextual analysis and scoring criteria (e.g. to assist with selecting reform targets and sequencing of activities);
- Repository of good practice examples at the country level;
- Identifying score gaps for entry points of policy reform (e.g. score gaps between legal frameworks and implementation; score gaps across policy areas and institutions, etc.).

Defence Transparency and the Civic Space of Defence: NATO Member Countries

Transparency is one of the basic principles of good governance. It entails that governments make records available to the public regarding their decision-making, policies, activities, and future plans in order for citizens to participate in policymaking and monitoring government activity. In the defence sector, national security interests and the public's right to access public information have frequently been at odds. Many states do not guarantee the public's access to any defence information whatsoever, while even in countries where legislation is in place to regulate this, the information that is made available is limited or superficial.

Civic space is the set of conditions that allow civil society organizations and individuals to organize, participate, and communicate freely and without discrimination, in order to co-create political and social structures for society.[16] Core civic space rights, such as freedom of association, freedom of assembly, and freedom of expression are the critical foundations for civil society to flourish and for civic space to be considered open. The

[16] Sam Perlo-Freeman, "Transparency and accountability in military spending," SIPRI, August 3, 2016, https://www.sipri.org/commentary/topical-backgrounder/2016/transparency-and-accountability-military-spending (accessed February 23, 2026).

'civic space of defence' refers to the capacity for civil society, media, and citizens to monitor, debate, and influence national security and military policies within a larger, open, civic space.

	Defence Transparency	Civic Space of Defence
Albania	49	39
Belgium	81	73
Canada	64	57
Denmark	65	80
Estonia	64	50
France	59	43
Germany	73	80
Greece	47	45
Hungary	44	27
Italy	69	61
Latvia	77	91
Lithuania	64	73
Montenegro	44	39
Netherlands	72	84
North Macedonia	70	66
Norway	84	84
Poland	58	57
Portugal	65	52
Spain	62	52
Türkiye	21	20
United Kingdom	84	86
United States	67	50

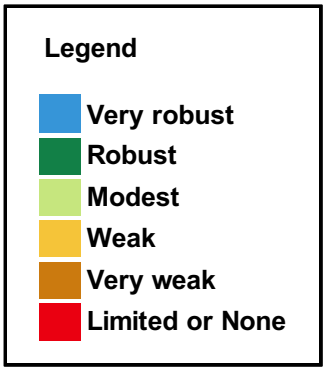


Figure 14.1: NATO Member Scores on Defence Transparency and the Civic Space of Defence.[17]

Defence Transparency

Defence is frequently cited as one of the most opaque areas of government activity, despite being an area of significant government expenditure. A lack of transparency undermines sound financial management of the sector and creates a high vulnerability to corruption. This is especially true in relation to procurement and defence sector expenditure more broadly.[18]

Recent analysis points to the finding that robust transparency in the defence sector is highest amongst states with more participatory and transparent government. This includes G7 members, North and Western European states, and countries classified as liberal democracies, some of which are the top arms exporters and military spenders in the world.[19]

[17] Transparency International Defence & Security, *GDI 2020 Global Report: Disruption, Democratic Governance, and Corruption Risk in Defence Institutions* (Transparency International Defence & Security, December 22, 2021), https://ti-defence.org/publications/gdi-2020-global-report-disruption-democratic-governance-and-corruption-risk-in-defence-institutions/. (Scores out of 100). There are 22 NATO member countries included in the 2020 GDI.
[18] Perlo-Freeman, "Transparency and Accountability."
[19] Transparency International Defence & Security, *GDI 2020 Global Report: Disruption, Democratic Governance, and Corruption Risk in Defence Institutions* (London: Transparency International UK, 2021).

If defence exceptionalism were a recurrent theme throughout defence establishments, the expectation would be to see defence transparency scores low across the whole index. However, this is not the case. A comparison of GDI scores with the World Justice Project Rule of Law Index reveals that countries with higher, more open governments, achieve higher scores on defence transparency.[20] The implication, therefore, is that weak transparency in defence is a political decision, not a necessity for national security.

No.	Defence Policymaking and Political Affairs	NATO average	Index average
30A	Legal Framework on Access to Information	76	49
21B	Legislative Access to Classified Information on Intelligence Services	63	45
3D	Transparency of Defence Strategy and/or Security Policy	61	41
11B	Transparency of Acquisition Planning	57	40
76C	Lobbyist Registration System	50	49
30C	Effectiveness of Access to Information	51	32
76B	Lobbying Disclosure: Public Officials	38	31

No.	Defence Finances	NATO average	Index average
77C	Timeliness of Disclosure on Defence Spending	93	74
12B	Timeliness of Budget Proposal	84	66
14B	Comprehensiveness of Budget Disclosure	78	54
12A	Comprehensiveness of Budget Proposal	76	60
14A	Proactive publication of Budget	76	53
77B	Comprehensiveness of Defence Spending Disclosure	76	63
31B	Beneficial Ownership of Commercial Businesses	73	46
15A	Transparency of Defence Income	72	45
77A	Proactive Publication of Defence Spending	69	45
14C	Response to Information Requests on Budget	68	42
17C	Access to External Audit Reports	66	58
24B	Transparency of Asset Disposal Process	61	38
25C	Transparency of Asset Disposals	56	38
77D	Explanation of Defence Spending Variances against Budget	56	36
27	Legislative Access to Information on Secret Spending Items	51	33
18D	Transparency of Military Involvement in Natural Resources	50	15
32B	Transparency of Military-Owned Businesses	50	29
24C	Transparency of Financial Results of Asset Disposals	49	28
16C	Legislative/Executive Access to Internal Audit Reports	48	40

No.	Defence Personnel Management	NATO average	Index average
46B	Transparency of Military Code of Conduct	90	76
39A	Transparency of Pay Rates	89	65
47B	Transparency of Civilian Code of Conduct	88	74
40C	Transparency of Payment System	81	52
39B	Transparency of Allowances	75	54

[20] *World Justice Project Rule of Law Index 2021* (World Justice Project, 2021), https://worldjusticeproject.org/our-work/publications/rule-law-index-reports/world-justice-project-rule-law-index-2021.

38B	Transparency of Defence Personnel Numbers	74	39
49B	Transparency of Corruption Prosecutions	69	44
42D	Frequency of Disclosure on Promotions	67	54
41C	Transparency of Appointments	63	34
49A	Transparency of Corruption Prosecution Policy	60	40
42C	Comprehensiveness of Disclosure on Promotions	43	35

No.	Corruption in Operations	NATO average	Index average
54C	Transparency of Corruption Monitoring in Operations	25	21

No.	Defence Procurement	NATO average	Index average
60A	Transparency of Potential Purchases	77	47
59C	Transparency of Procurement Oversight	71	44
65C	Transparency of Tender Board Controls	70	48
58B	Transparency of Procurement Cycle	61	39
65B	Audit Trail of Tender Board	61	38
61A	Comprehensiveness of Disclosure on Actual Purchases	58	37
60B	Notice of Planned Purchases	53	29
61B	Accessible Data on Actual Defence Purchases	53	33
67B	Transparency of Contract Awards	44	24
62A	Transparency of Policies on Business Compliance Standards	39	25
73A	Transparency of Policies on Agents and Intermediaries	36	28
74	Transparency of Financing Packages	25	12
71B	Transparency of Offset Contract Monitoring*	19	10

Figure 14.2: Defence Transparency Scorecard for NATO Member Countries.

A key legislative tool for facilitating transparency is access to information. These are laws that enshrine the right of citizens to view information on the functioning of their governments and that create an obligation for governments to either provide the information, or justify why they cannot.[21] Effective access to information systems requires robust legal frameworks, responsive institutions, enforceable and realistic sanctions, and strong information management processes.[22]

GDI data reveals that nearly half of the countries in the index are 'modest' to 'very robust' in their access to information regimes, with even more countries having a well-designed law in place. However, there is a clear gap between legal frameworks and implementation, reflected in the data for NATO countries, shown in Figure 14.3. Although over half of the NATO countries in the index have top scores on the quality of their legal frameworks for ATI, only one country has top scores in implementation, and only five with scores above 50. In an area as sensitive as defence, where information is often closely guarded, enacting governing legislation has proven complicated. National security and the public's right to information have historically been viewed as 'pulling in

[21] Stephen Kosack and Archon Fung, "Does Transparency Improve Governance?," *Annual Review of Political Science* 17, no. 1 (2014): 65–87 at 67, https://doi.org/10.1146/annurev-polisci-032210-144356..
[22] Victoria Lemieux and Stephanie Trapnell, *Public Access to Information for Development: A Guide to Effective Implementation of Right to Information Laws* (Washington, DC: World Bank, 2016), https://doi.org/10.1596/978-1-4648-0879-1.

opposite directions,'[23] with defence institutions' 'secrecy privilege' on one side and those advocating for a 'transparency fix' on the other.[24]

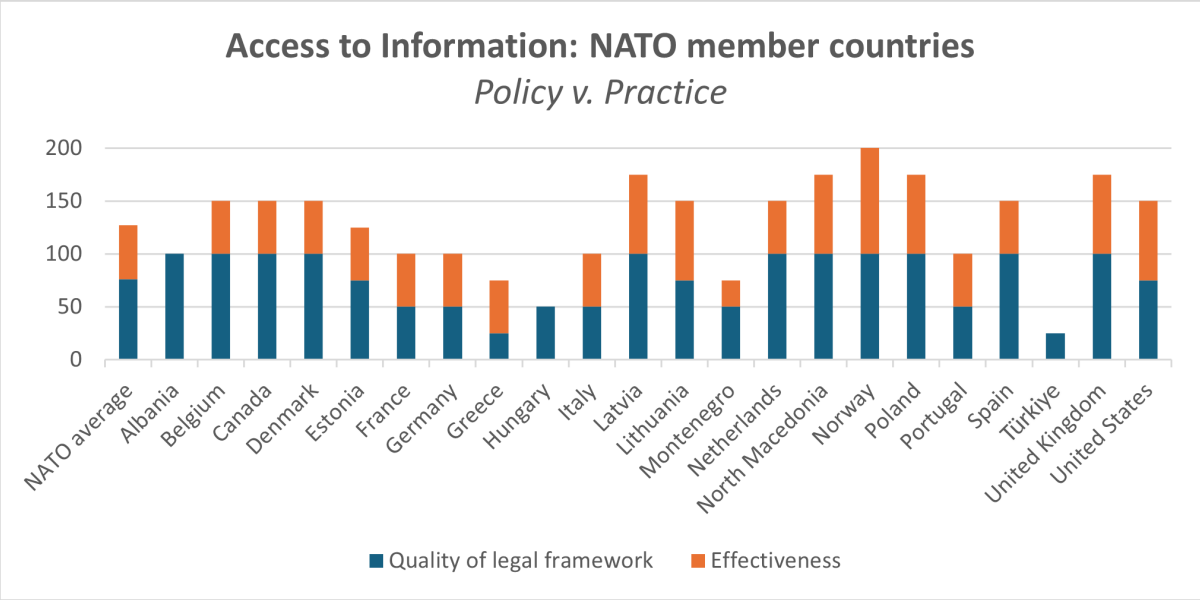


Figure 14.3: NATO Member Country Scores on Access to Information.

However, transparency and secrecy can each contribute to national security, both by protecting information crucial to the security needs of the state and by ensuring that the cloak of secrecy is not used to hide irregularities, abuses of power, or fraud. Decisions to restrict access to information must balance the public interest with the harm that releasing specific pieces of information could do, and be based on well-justified exceptions that preserve the overall presumption of transparency and access to information. Overclassification itself is a dangerous practice, which leads to the dilution of classification standards and the deterioration of the classification system as a whole. Transparency is critical for the governance of public functions, as well as serving as the foundation for public trust and a robust civic space.

The Civic Space of Defence

Engagement between civil society and defence institutions is often limited due to: a tradition of secrecy; the prioritization of national security concerns over civil liberties; the technical nature of the defence sector; and the lack of trust between civil society and defence institutions. In the current global context marked by shrinking civic space,[25] particularly in a post-pandemic world, it is more important than ever to ensure that civil society has the space and freedom they need to voice their concerns and bring their expertise to the table.[26]

[23] Open Society Justice Initiative, *Global Principles on National Security and the Right to Information* ('Tshwane Principles') (Tshwane, South Africa: Open Society Justice Initiative, June 12, 2013), https://www.justiceinitiative.org/publications/global-principles-national-security-and-right-information-tshwane-principles.
[24] Mark Fenster, *The Transparency Fix: Secrets, Leaks, and Uncontrollable Government Information* (Stanford, CA: Stanford University Press, 2017), pp. 9–11.
[25] Saskia Brechenmacher and Thomas Carothers, *Defending Civic Space: Is the International Community Stuck?* (Washington, DC: Carnegie Endowment for International Peace, October 2019), https://carnegieendowment.org/research/2019/10/defending-civic-space-is-the-international-community-stuck.
[26] Colin Anderson, Andy Sumner, and Tingting Xu, *Navigating Civic Space in a Time of Covid: Synthesis Report* (Brighton: Institute of Development Studies, May 2021), https://doi.org/10.19088/A4EA.2021.002.

No.	Civic Space Indicator	NATO average	Index average
4B	Protections for Civil Society Organizations	80	54
6A	Public debate around Defence Issues	72	57
14C	Response to Budget Information Requests	68	42
3A	Range of Actors Involved in Defence Policy Debate	65	46
3B	Scope of Defence Policy Debate	64	52
6B	Extent of Government Engagement in Public Discourse	64	46
3D	Transparency of Defence Policy Documents	61	41
4C	Practice of openness to Civil Society Organizations	50	36
4A	Policy of Openness to Civil Society Organizations	49	32
3C	Public Consultations in Defence Policymaking	43	29
15C	Public Scrutiny of Defence Income	40	27

Figure 14.4: Civic Space of Defence Scorecard for NATO Member Countries.

Openness of Defence Institutions

A key factor in robust civic space is the government's openness to engaging with civil society. If this is limited, then the quality of dialogue on policy and strategic issues, and the effectiveness of participatory mechanisms, are also likely to be limited. The government and defence institutions can easily withdraw from these processes. As such, civil society might find themselves walking a tightrope. They want to engage fully and frankly on defence issues, but they also do not want to be shut out completely by defence actors – or worse, become targets for harassment and intimidation.

Findings for NATO member countries are extremely varied on the openness of defence institutions to civil society. Data reveals that many NATO countries have weak policies on engagement, but score well in terms of practice. Only seven countries score above 50 on the presence of a policy. In five countries, there is a complete absence of any policy (Denmark, France, Greece, Hungary, Türkiye), with two countries having no engagement (Greece and Türkiye). Latvia, Netherlands, and North Macedonia are the only countries to score highly on both the policy and practice of civil society engagement. While the practice of openness is critically important, it is also vital to have a policy that defines the terms of engagement, so that civil society actors have a framework through which to engage the MoD.

General Public Discourse on Defence v. Specific Defence Policy Discussions

GDI data sheds light on a clear gap between a broad public debate on issues of defence, and the prevalence of more specific engagement with defence institutions on policy or security strategy. When debate does occur, in many cases the executive is not involved and discussion is confined to the media and civil society.[27] This dilutes the potential impact of these debates and underlines how disengaged the executive can be with civil society and with consultative policymaking in general, in the field of defence.

[27] Transparency International Defence & Security, *GDI 2020 Global Report: Disruption, Democratic Governance, and Corruption Risk in Defence Institutions* (London: Transparency International UK, 2021), https://ti-defence.org/wp-content/uploads/2021/12/TI-GDI-Global-Report-v7.pdf.

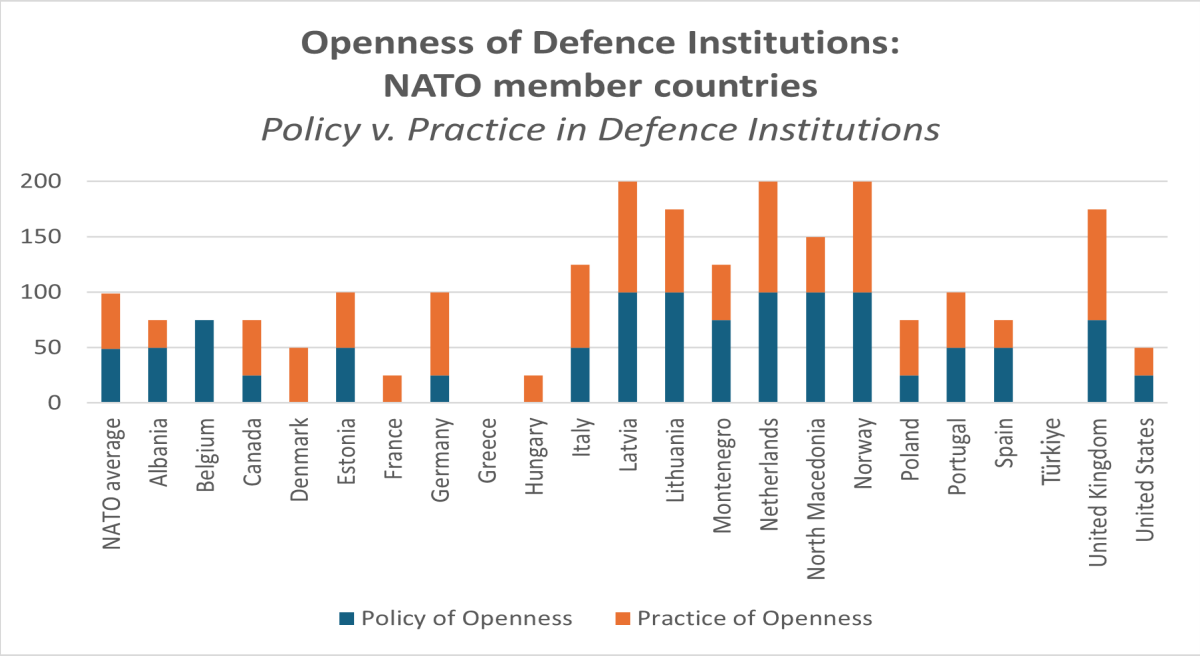


Figure 14.5: NATO Member Country Scores on the Openness of Defence Institutions.

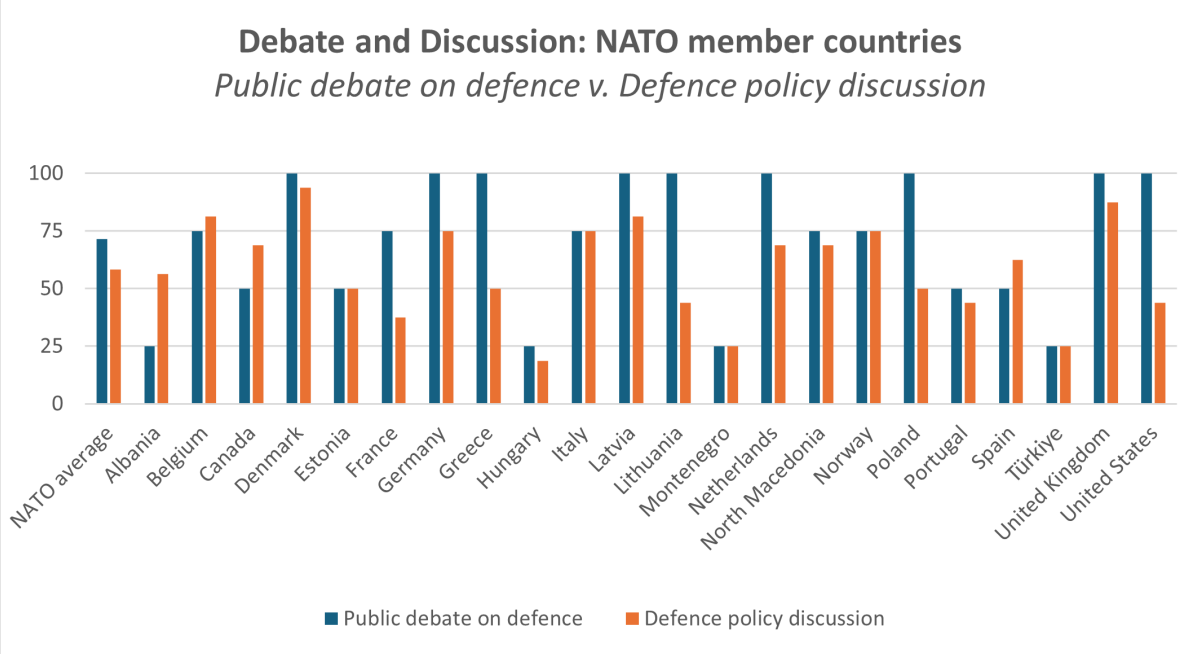


Figure 14.6: NATO Member Country Scores on Defence Debate and Policy Discussions* *Public debates on defence may be wide-ranging in scope, often attending to scandals, and tackling issues such as integrity and effectiveness, while defence policy discussion focuses on defining the means that would allow a nation to deal effectively with likely future threats and challenges.*[28]

NATO member countries generally have modest to robust public debate on defence issues, as well as defence policy discussions. But in half the countries, there is a clear decline from broad debate to specific engagement of civil society, which in some cases constitutes more than a fifty-point drop.

[28] Todor Tagarev, "Formulating Defense Policy: Main Considerations and Evaluation Criteria," *Connections: The Quarterly Journal* 24, no. 3 (2025), https://doi.org/10.11610/Connections.23.4.12.

Consultative Processes

Regular consultations and access by civil society to information on the defence policy and/or security strategy constitutes another form of accountability to the public. Public discussions feed into dialogue between civil society and policymakers, who can then incorporate findings into policymaking processes. In fact, the engagement of civil society as a 'watchdog' and barometer of contentment with institutional performance makes it integral to good governance and accountability.[29]

Across the index, the level of public discussions on national security strategies and defence policies is very low, with a global score of 29/100. This suggests that broader public engagement is required in order to strengthen defence policymaking. In fact, only three countries score in the top bracket: Malaysia, Sweden, and New Zealand. Conversely, 47% of countries in the index have had no formal consultation process involving the public in defence policy formulation in the last five years.

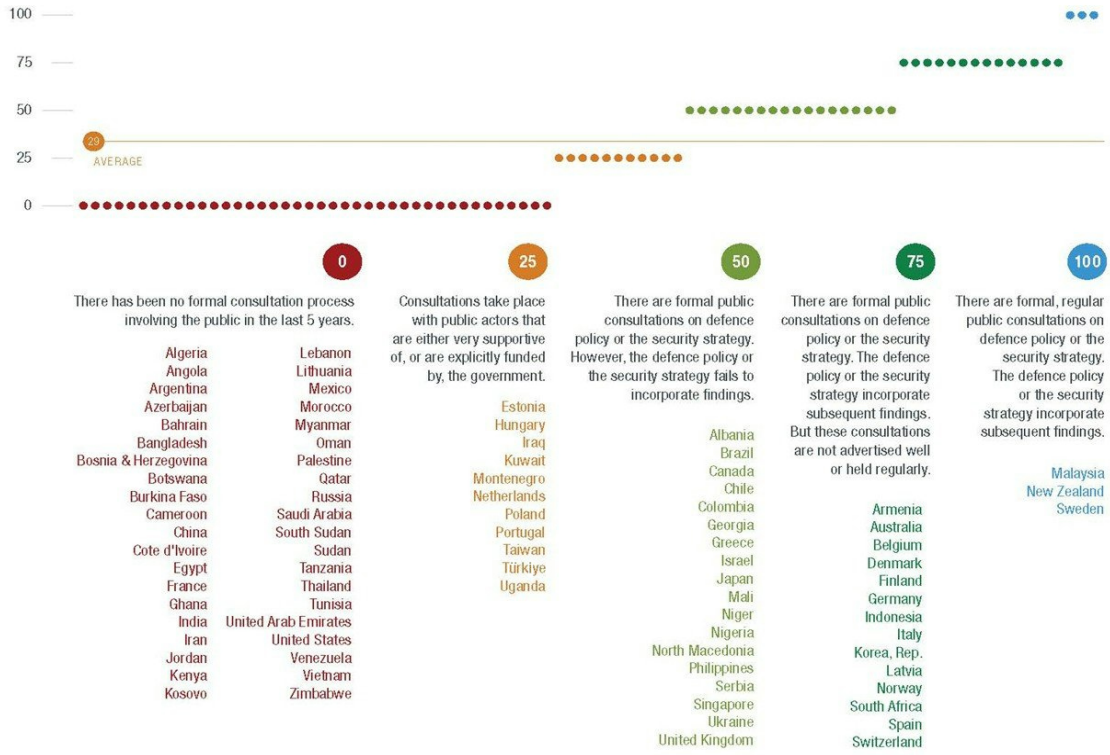


Figure 14.7: GDI scores on the prevalence of consultations in the defence sector.

Of NATO member countries, three have not held any formal consultations on defence issues in the last five years (France, Lithuania, and the United States). Only seven NATO member countries hold consultations, but not regularly. The remainder either fail to incorporate consultative findings or invite public actors that are supportive of, or financially supported by, the government. Though these findings are not necessarily indicative of weak consultative processes, it must be countered by engagement with a range of actors outside the main policy circles of defence institutions.

[29] United Nations Development Programme (UNDP), *Public Oversight of the Security Sector: A Handbook for Civil Society Organizations* (New York: United Nations Development Programme, 2008), https://www.undp.org/sites/g/files/zskgke326/files/publications/2008_UNDP_CSO-Handbook-Public-Oversight-of-the-Security-Sector-2008.pdf.

There is successful work being done in Tunisia regarding consultative and monitoring entities in the defence and security sector: the Tunisian Ministry of Defence have engaged with the Transparency International (TI) chapter in Tunisia, IWATCH, as well as TI-DS, in relation to the past two iterations of the GDI. Over the past 5 years, IWATCH have made defence one of their key areas of work and are now the main authority within Tunisian civil society on transparency and integrity in the defence sector. As well as continuing to work directly with the MoD to support their governance reform efforts, they have established a monitoring group (the Collective for Defence and Security Integrity) composed of experts from across Tunisian civil society. This group's role is to produce evidence and policy positions in relation to governance reforms needed in the defence sector, to provide external oversight of the Tunisian defence sector, and to advocate for greater transparency and stronger anti-corruption controls in defence.

Conclusion

Neither transparency nor civic engagement is sufficient for consequential governance outcomes. But robust civic space and freedom of expression are critical prerequisites for democracy, and serve as safeguards against war and conflict.[30] Robust transparency, combined with effective oversight and meaningful civil society engagement, thus becomes a crucial means of improving governance and reducing corruption risk in the defence sector.[31]

[30] Norwegian Nobel Committee, "The Nobel Peace Prize 2021," press release, October 8, 2021, https://www.nobelprize.org/prizes/peace/2021/press-release/ (accessed February 23, 2026).
[31] For correlations with democracy, transparency, and governance, as well as further discussion, see: Transparency International Defence & Security, *GDI 2020 Global Report: Disruption, Democratic Governance, and Corruption Risk in Defence Institutions* (London: Transparency International UK, 2021), https://ti-defence.org/wp-content/uploads/2021/12/TI-GDI-Global-Report-v7.pdf.

Part 5: Organizing Building Integrity Initiatives

This section moves from explaining corruption risks in defence to showing how organizations can systematically respond to them. The first article introduces corruption risk assessment as a method or identifying vulnerabilities, prioritizing action, guiding policy and institutional reform. The second chapter turns to implementation, outlining how building integrity programmes help defence organizations institutionalize ethical practices through governance principles, performance management, and measurable outcomes. Finally, a case study on Luxembourg illustrates how integrity is also strengthened through values-based culture building, showing how collaborative ethics processes, codes of conduct, and leadership engagement can transform identity and behaviour. This part shows that fighting corruption is not simply about detecting wrongdoing. It requires structured programming, sustained leadership, and values that bind organizations to their mission.

15.Mapping Corruption Risks

Prof. Todor Tagarev, Dr. Michael Ofori-Mensah, and Denitsa Zhelyazkova

The preceding chapters provide numerous examples of the vulnerabilities of defence organizations and how they are being or could be exploited for corrupt activities. A defence leader might easily be overwhelmed by the scale of the integrity building task. Therefore, to not waste organizational resources and political capital in an attempt to address all these vulnerabilities, leaders need to understand the main issues. In the policy-making and management literature and practice, this means grasping the major corruption risks in the current context and focusing integrity building efforts accordingly. That implies follow-on actions for elaborating and assessing the potential effects of risk mitigation measures, including the selected measures in a corruption risk response plan, designating risk owners and officials responsible for their implementation and oversight – all in a routine cycle of review and assessment.

This chapter introduces the concept of risk and selected tried approaches for assessing and visualizing risks. It includes examples and guidelines on mapping corruption risks in defence and security sector organizations. Corruption risk assessment facilitates policymaking as it provides a clear picture of high-risk areas. This method is especially beneficial when employed in long-term programmes like NATO BI. Despite the voluntary nature of the programme, activities, such as specialized training access or self-assessment, could be even more effective when targeting high-risk areas alone.

Introduction to the Concepts of Risk, Corruption Risk, and Risk Assessment Methodologies

The ISO standard 31000:2018[1] defines 'risk' as the 'effect of uncertainty on objectives.' Generally, the deviation from the expected can be negative or positive and may lead to opportunities or threats. Risk is usually expressed in terms of *risk sources*, potential *events*, their *consequences,* and their *likelihood*. Transparency International (TI) defines corruption risk through 'the set of institutional vulnerabilities within a system or process which might favour or facilitate corrupt practices.'[2] Thus, the sources of risk are vulnerabilities and actors, willing to exploit them, the 'event' is the act of corruption, and the effect is negative. As pointed out by ISO 31000, the *consequences* can be certain or uncertain and can have direct or indirect effects.[3] They can be expressed qualitatively or quantitatively, and escalate through cascading and cumulative effects. '*Likelihood*' is used to refer to 'the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.'[4]

In some fields, for instance assessing flood risk, there is abundant quantitative historical data. However, due to its clandestine nature, evaluating corruption risk by looking at patterns in known or suspected cases is a complex and often challenging task. This is especially so in the secretive context of the defence sector. There are several different approaches to conceptualizing corruption risk. It could be defined as the set of institutional weaknesses within a system or processes that facilitate corrupt practices.[5] An understanding of risks can be usefully enhanced by exploring data on perceptions and/or experience of corruption. Depending on the context-specific evaluation tool and the focus of the study, corruption risk can also be perceived as the factor of the likelihood of corruption multiplied by its consequences.[6] Some authors have also examined risk through the lens of transparency and

---

1 International Organization for Standardization, ISO 31000:2018(en) *Risk management — Guidelines*.

2 Andy McDevitt, *Gateway Corruption Assessment Toolbox: Corruption Risk Assessment Topic Guide* (Transparency International, 2011), https://knowledgehub.transparency.org/assets/uploads/kproducts/Corruption_Risk_Assessment_Topic_Guide.pdf.

3 International Organization for Standardization, ISO 31000:2018(en) *Risk management — Guidelines*.

4 Ibid.

5 McDevitt, *Gateway Corruption*.

6 "Rationale and Outline of a Corruption Risk Assessment," Paper for Comment and Decision (Council of Europe, 2019), https://rm.coe.int/eccd-cra-methodology-proposal-en/168098f194.

fairness, while others argue that corruption risk can be expressed as the difference between actual and ideal systems.[7]

There are several strategies for conducting corruption risk assessments. The compliance-based approach focuses on anti-corruption laws and sanctions, while the integrity or value-based methodology examines the public service/ private sector ethical values and perceptions as well as the effectiveness of integrity management.[8] In comparison, applying a risk-based approach in preventing and fighting corruption is, to an extent, a combination of the aforementioned methods. The approach involves a rigorous understanding of institutional resilience. This means identifying potential gaps in the existing legislature and state mechanisms, thus focusing all efforts and resources on fewer but essential targets with the aim of establishing a long-term anti-corruption strategy.[9] In this way, measuring corruption by assessing corruption risk is integral to drawing conclusions on the nexus between contextual actors and specific risks.

Depending on the definition of corruption risk, the notion can be evaluated through several methods, which are often employed together through: (i) surveying public perceptions on how corrupt the authorities are and/or how many people have experienced any form of corruption; (ii) expert assessments; (iii) looking at case studies and seeking proxies based on available data.[10] All three methodologies have their limitations. Exploring public perceptions is often argued to be a misleading representation of real corruption risk. How those perceptions are collected and analysed creates, in turn, a new set of methodological caveats. This includes: bias of both participants and surveyors; survey design; and weighting of factors for the analysis.[11]

Similarly, expert assessments can be the subject of potential bias not only through the decision on the number of experts needed, but also *via* the transparency of the selection process itself. The risk-based approach relies heavily on available data. However, clarity on corruption cases is rare, especially when focusing on specific types of corruption in the secretive context of the defence sector. Therefore, the scarcity of data on corruption cases renders this approach contingent on using triangulated data to assess corruption risk. It is also important to note here that some scholars criticize composite indicators when measuring corruption risk. They argue that different types of corruption cannot be thoroughly examined at the aggregate level, which in turn renders all efforts to provide national-level statistics on corruption futile.[12]

To briefly illustrate the points above, TI's Corruption Perception Index (CPI) aggregates data from 13 different sources. These provide perceptions by business executives and country experts *vis-a-vis* the level of corruption in the public sector. The diversity of sources aims to explore different types of corruption and avoid any respondent and assessor's bias. There is a clear and detailed methodology paper. However, one potential critique to this approach is that it looks at corruption as a composite in the results, and thus risks focusing on only one side of an otherwise multifaceted phenomenon. Despite the arguments against utilizing public perceptions

---

7 United Nations Economic Commission for Europe, *Governance Analysis Toolkit for Customs and Border Management*; Liljana Selinšek, *Corruption Risk Assessment in Public Institutions in South East Europe* (Regional Cooperation Council, 2020).

8 Zeger van der Wal, Adam Graycar, and Kym Kelly, "See no Evil, Hear no Evil? Assessing Corruption Risk Perceptions and Strategies of Victorian Public Bodies," *Australian Journal of Public Administration* 75, no. 1 (2016): 3-17, http://dx.doi.org/10.1111/1467-8500.12163; Ting Gong and Sunny L. Yang, "Controlling Bureaucratic Corruption," *Oxford Research Encyclopedia of Politics*, June 25, 2019, https://doi.org/10.1093/acrefore/9780190228637.013.1463.

9 Transparency International, *Procurement Risk Map*.

10 Anuradha K. Rajivan and Ramesh Gampat, *Perspectives on Corruption and Human Development* (Colombo: United Nations Development Programme, Regional Centre for Asia Pacific, 2009); Finn Heinrich and Robin Hodess, "Measuring Corruption," in *Handbook of Global Research and Practice in Corruption*, edited by Russel G. Smith and Adam Graycar (Cheltenham: Edward Elgar Publishing, 2011), pp. 18-31.

11 Andersson, Staffan, and Paul M. Heywood, "The politics of perception: use and abuse of Transparency International's approach to measuring corruption," Political Studies 57, no. 4 (2009): 746-767; Paul Heywood, "The Corruption Perceptions Index (CPI): the Good, the Bad and the Ugly," *The British Academy*, 2016, https://www.thebritishacademy.ac.uk/blog/corruption-perceptions-index-cpi-good-bad-and-ugly/.

12 Matthew Stephenson, "Are Aggregate Corruption Indicators Coherent and/or Useful?: Further Reflections," Global Anticorruption Blog, 2016, https://globalanticorruptionblog.com/2016/10/04/are-aggregate-corruption-indicators-coherent-andor-useful-further-reflections/.

surveys, TI's global survey, the Global Corruption Barometer,[13] assesses experiences with corruption as well. Similar experience-based tools provide a more reliable platform to evaluate risk based on public experiences with corruption.

This chapter will provide three examples of corruption risk assessment and mapping. The first example is TI's Government Defence Integrity Index (GDI). GDI measures corruption risk by probing institutional resilience to corruption in national defence establishments. The GDI assesses both legal frameworks and applications, as well as civic space, parliamentary oversight, financial resource and personnel management, thus capturing the implementation gap between law and practice. The guidance of the French Anti-Corruption Agency provides the second example The third example presented below is the corruption risk mapping in Bulgaria's Ministry of Defence (MoD). Another example is the Defence Companies Index on Anti-Corruption and Corporate Transparency (DCI), also published by TI.[14] It assesses the levels of public commitment to anti-corruption and transparency in the corporate policies and procedures of 134 of the world's largest defence companies by also providing a framework of good practice.

Transparency International Government Defence Integrity Index

As mentioned previously, measuring corruption risk in the defence sector is exceptionally challenging. It requires a mixed methodology that combines: (i) thoroughly selected experts; (ii) continuous oversight of the data collection process to avoid perceptions bias; (iii) comprehensive survey design ensuring a detailed wide-reaching dataset, and (iv) strict good practice guidelines to facilitate the analysis of the results. The GDI index examines corruption risks in national defence establishments by critically evaluating the framework of institutional resilience and providing a framework of good practice that promotes transparent and accountable defence governance.

The GDI's objective is not to measure corruption, examine the amount of lost funds on a case-by-case basis, identify corrupt actors, or assess perceptions of corruption by the general public. Rather, the GDI is a corruption risk assessment of the defence and security sectors within a country, which examines the quality of mechanisms used to manage corruption risk through the prism of transparency, oversight and civic space. The index focuses primarily on internal issues and, thus, adopts a tailored approach when evaluating state-specific structures and mechanisms. There are only a few questions being applicable to the country's external impact through arms exports and military operations.

Depending on the purpose of the exercise, the methodology used, context-specific mechanisms and actors as well as the timeline and available resources, corruption risk assessments vary enormously. Therefore, there is no universal formula on conducting a risk assessment in the defence sector. However, there are some general steps that can be undertaken and tailored to the targeted sector needs and governance objectives.

GDI Risk Assessment Process[15]

Stage 1: Ensure continuous expert commitment, oversight and guidelines. The collection of data, especially using a mixed methods approach might be an arduous and time-consuming task. Hence, the researchers/assessors/peer reviewers need to be selected carefully, ensuring long-term commitment and rigorous guidelines on what is acceptable and what is not, including oversight measures.

Stage 2: Plan, scope and mobiliZe. For the planning phase, it is essential to consider:

[13] Transparency International, *Global Corruption Barometer: European Union 2021* (Transparency International, June 15, 2021), https://images.transparencycdn.org/images/TI_GCB_EU_2021_web.pdf.

[14] Transparency International Defence & Security, *Defence Companies Index on Anti-Corruption and Corporate Transparency*, https://ti-defence.org/what-we-do/industry-integrity/defence-companies-index/.

[15] Adapted from TI's Global Anti-Bribery Guidance, https://www.antibriberyguidance.org/.

- Methodology and the preparations surrounding it (e.g. for interviews with defence sector officials – location, structure, translations, etc.);
- Methodological limitations;
- Responsibilities of everyone involved in the exercise, from the researchers, interviewers and peer reviewers to context-specific assessors, interviewees or survey respondents;
- Oversight guidelines;
- Timeline;
- Communication plan;
- Project risks (e.g. no access to data on defence budgets and spending; unsuccessful development of partnerships, adverse reaction from government, etc.)

Stage 3: Collect data. Depending on the contextually conceded concept of the corruption risk, gathering the data will vary significantly from one project to another.

Stage 4: Identify the risks. After collecting the data, the next step is to select the best approach to examine the data and identify any high-risk areas or feasible correlations.

Stage 5: Evaluate and prioritize the risks: This stage analyses and prioritizes any gaps in legislature and practice identified in step 3, taking into account the risk factors identified in step 4. It is common practice to examine two variables in prioritizing the risks: the likelihood of occurrence and the potential adverse impact.

Stage 6: Use the output of the assessment: The results are then applied to either review or amend current anti-corruption measures. This includes: training; oversight procedures; civic involvement; etc. The variables from step 5 can be visually assessed through risk mapping (see more details below).

Box 15.1: Key Roles in Assessing Corruption Risks

The core of the GDI methodology consists of a lead *Country Assessor* scoring and answering the questionnaire. The survey focuses on 29 corruption risk areas relevant to the defence and security sectors. Assessors are expected to conduct both desk research and interviews with key individuals in government, military, academia, and civil society, allowing for confidentiality to protect the safety of informants. As the scores are a result of mixed methods analysis, with both quantitative and qualitative data and a heavy reliance on narrative justification, it is imperative that evidence is properly cited and triangulated for accuracy and objectivity. Assessors are expected to adhere to the following standards for data collection:

- Qualitative data must be original. Explanatory text must be context-specific, and well-evidenced. There must be a defensible and balanced judgment to justify the score of each indicator;
- The narrative justification is, as far as possible, objective, and takes into account the sources used as evidence. Multiple perspectives are encouraged where an issue is controversial or risks a subjective reading;
- The text must be qualified. When the information presented is the opinion of an interviewee or a reflection of public opinion, this must be made apparent. The reliability of all subjective opinion is examined. These sources are evaluated critically, and information provided is verified with other sources;
- Responses are supported by at least two recent sources, except in the cases of *de jure* indicators, such as where there is only one piece of guiding legislation. If only one source is retrieved, the circumstances need to be explained. A lack of evidence for something might indicate a lack of transparency, which in itself implies a higher corruption risk. In some cases, responses require proving a negative, requiring thorough desk and interview research.

The entire research process for one country lasts about 12 to 14 months from the launch of data collection to the publication of results. At each stage, TI-DS conducts comprehensive checks for coherence of explanations, justification for scores, and adequacy of evidence. Once completed, the assessment is sent to two independent peer reviewers for review and comment as part of the drafting process. Peer reviewers are asked to check and validate the assessor's research, while providing insights based on their expertise. Peer review comments are considered part of the drafting and revision process for the GDI assessment. Assessors are expected to respond to all peer reviewer comments, either by integrating the information into the assessment as appropriate, or by explaining why the assessment need not be amended in light of reviewer comments.

GDI Country Assessors: Selection Process

The selection process for country assessors is meticulously structured and executed. The assessors are carefully selected on the basis of their relevant skills and experience. They are usually PhD-level researchers, journalists, and specialists with proven experience in conducting primary and secondary research, collecting and analysing quantitative and qualitative data with a specific focus on carrying out interviews. The assessors are ideally selected to be local sector specialists who understand how to access pivotal information (including data available only in one language) and they have the necessary networks to source relevant interviewees. To be able to discern the difference between evidence/facts and perceptions/ opinions, the experts are not only examined through several rigorous rounds of interviews, but they also must present a writing sample to the interviewing board. The article must follow the high standard of GDI index country assessments from previous years. This enables the board to detect any potential political bias from an early stage and allows them to make the right decision as to whether the candidate is suitable for a role that requires high ethical and professional standards. After the successful appointment, the assessors might wish to remain anonymous as a safety measure depending on the country-specific context.

GDI Peer Reviewers:

The two peer reviewers are also selected through a scrupulous and well-structured process. They are selected on the basis of being experienced and well-respected academics within their field and, similar to the country assessors, their skills are also tested *via* a combination of interviews and written work. Both positions require not only field expertise, but also high ethical standards to which the peer reviewers must adhere at all times. With proven expertise on the subject matter, the peer reviewers also need to have in-depth knowledge about the defence sector in the assessed country. This, in turn, enables them to point out context-specific weaknesses in the quality of evidence or the accuracy of scores. The reviewers are indeed a focal point for building the high-standard work on GDI index country assessments. The experts examine the collection of data periodically and return comments back to the country assessors for amendments until the content for analysis is of impeccable quality, while TI-DS oversees the whole process.

GDI: Governments Feedback

An integral part of the GDI research process is the involvement of governments in verifying the accuracy of data in their country assessments and in providing additional commentary or evidence to justify scores. All governments from countries in the index are formally invited to appoint a reviewer to work with TI-DS on a thorough review of the assessment. Their comments are evaluated and incorporated where relevant. Governments are also invited to submit a formal statement on GDI findings, which will be posted online with country data. In addition, each nationally-based TI chapter is provided with the GDI findings for their country in order to verify accuracy and provide commentary. Norway and Switzerland are among the countries that reviewed their draft GDI findings and provided detailed comments on questions and scores.

The next section offers a brief, yet general guide based on good practice that can serve to complement and adapt the GDI approach to corruption risk assessment.

Corruption Risk Mapping Guidance of the French Anti-Corruption Agency

Despite the lack of a universal definition/tool, corruption risk assessment is a unique approach, which examines institutional susceptibility and vulnerability by probing the prospect of corruption occurring and its potential impact. The last step in the process entails a rigorous study of how specific state mechanisms function through a detailed mapping of all governance components. Risk mapping is, thus, a useful tool to visually explore the correlation between likelihood and impact.[16] The process can be defined as the action of identifying, assessing, prioritizing and managing corruption risks,[17] aiming to ensure that anti-corruption measures are concentrated in high-risk areas. Exploring risk in terms of the likelihood of corruption occurring and its impact (severity), risk mapping enables a comparative assessment between state-specific defence structures and activities. That is, indeed, why a tailored local approach is pivotal when it comes to conducting corruption risk assessment. Diverse state institutions carry varying degrees of authority and responsibilities, hence country-specific regulations, as well as institutional vulnerabilities, may differ case by case.

There is no universal formula on how to conduct risk mapping. However, the French Anti-Corruption Agency (FACA) suggests the following six general steps: [18]

1. *Clarification of roles and responsibilities*: The mapping process ought to begin by identifying clearly defence officials who are responsible for the oversight procedures, thus setting the layout for the mechanisms already in place;
2. *Identifying risks*: This step involves a thorough examination of the data collected during the first stages of the assessment, followed by a classification of the specific risks;
3. *Assessing exposure to risks*: FACA refers to this step as the calculation of the 'gross' risk, i.e. how vulnerable the sector is, regardless of existing anti-corruption measures. FACA also recommends including an appendix to elaborate on the methodology used to calculate the 'gross' risks. This can include any definitions, as well as risk identification and classification procedures.

The agency also suggests that the following components are adopted when evaluating vulnerability:

1. *Analysis of risk factors, e.g. lack of legislation on the specific topic; no assigned compliance department; conflict and instability; etc.;*
2. *Determination of probabilities by looking at the most comprehensive and appropriate information for the specific nature of the identified risk (e.g. frequency of past incidents and their impact);*
3. *Assessment of aggravating factors and/or extenuating circumstances 19 by applying risk coefficients;*
4. *Additionally, TRACE International recommends refining the mapping methodology during this stage.*

Example:

To follow the formula below

Estimated Corruption Risk = Probability (likelihood) of risk occurring x Impact (severity) of risk occurrence x any applicable coefficients for aggravating or extenuating circumstances

16 World Customs Organization, *Guide to corruption risk mapping*, June 2015, http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/integrity/instruments-and-tools/risk_mapping_guide_june_2015.pdf?la=en.

17 "French Anti-Corruption Agency Guidelines," *Agence Française Anticorruption*, December 22, 2017, https://www.agence-francaise-anticorruption.gouv.fr/files/2018-10/French_Anticorruption_Agency_Guidelines.pdf.

18 "French Anti-Corruption Agency Guidelines," Agence Française Anticorruption, December 4, 2020, https://www.agence-francaise-anticorruption.gouv.fr/files/files/French%20AC%20Agency%20Guidelines%20.pdf.

19 TRACE International, *A Guide to Corruption Risk Assessment and Risk Mapping* (TRACE, 2021).

where the assessment of risk involves:

- Choosing between qualitative narrative-based or quantitative approach;
- Selecting a scale for likelihood and impact: e.g. quantitative approach can benefit from a five-point scale where 1 is '*rare*' and 5 is '*almost certain*' for likelihood; similarly, 1 can be equated to '*insignificant*' impact, while 5 can be assigned as '*critical*';
- Calculating the estimated risk following the formula above;
- Exporting results into a matrix that can be the first draft for a heat map, where the high-risk areas are highlighted in red (see Figure 15.1 below);

PROBABILITY (in the next 12 to 24 months)								
	> 90%	Almost certain	5	5	10	15	20	25
	50-90%	Likely	4	4	8	12	16	20
	20-50%	Possible	3	3	6	9	12	15
	5-20%	Unlikely	2	2	4	6	8	10
	< 5%	Rare	1	1	2	3	4	5
				1	2	3	4	5
				Insignificant	Minor	Moderate	Major	Critical
				IMPACT				

Figure 15.1: TRACE, A Guide to Corruption Risk Assessment and Risk Mapping (2021).

- Assessing current measures: Referring to the definitions from the previous point, this step entails computing the 'net' risk – taking into consideration the effectiveness of the mechanisms already in place. There are, of course various approaches to calculate that, but FACA recommends the following table:

Table 15.1. Assessing the Availability and Effectiveness of Currently Applied Risk Mitigation Measures.

	Systems	
	Structure	Effectiveness
Processes	• Absent • Under development • In place, but incomplete • In place	• Absent • Under development • In place, but ineffective or inappropriate • Effective and reliable
Procedures	• Absent • Under development • In place, but incomplete or out of date • In place, complete and up to date	• Absent • Under development • In place, but ineffective or inaccessible • Effective and enforced
Controls	• Absent • Under development • In place, but incomplete or out of date • In place, complete and up to date	• Absent • Under development • In place, but ineffective or inappropriate • Effective with > 80% success rate

- Prioritizing 'net' risks: identifying areas, where there are no control mechanisms in place or discerning clear patterns of implementation gaps between law and practice, ought to be prioritized. This process can also be included in the appendix with a clear framework on the prioritization process.

- Formalizing the map: the final step of the risk mapping process is formalising the final results and setting guidelines on updating the map as risk mapping is beneficial only when the exercise is repeated.

Box 15.2: Risk Assessment Tool Impact: GDI

Lebanese Armed Forces suggest creating an internal anti-corruption unit

Following the launch of the 2020 GDI findings for Lebanon, TI-DS held, in February 2020, a Leadership Day and Strategy Workshop with senior officials within the Lebanese Armed Forces (LAF) to present the GDI results. During this event, the LAF were clearly committed to anti-corruption efforts but openly admitted to lack of resources, expertise and mandate to implement the GDI's recommendations. As a solution, the LAF proactively suggested creating an internal anti-corruption unit with the mandate to improve integrity across the institution. In August 2020, the national chapter was in the process of researching and understanding the practicalities of setting up such a unit and intended to share their findings with the LAF to inform the unit's creation.

UK anti-corruption policy influenced by the GDI

As well as embedding transparency and anti-corruption in UK and NATO doctrine and training, and the work done with the UK Defence Academy, the British MoD publishes a guide to Corporate Standards. As well as addressing general standards of behaviour, it includes a section on Combating Fraud, Theft, Bribery and Corruption. TI-DS had substantial input into the current edition which was republished in 2025. The Foreword under the joint signature of the Chief of Defence Staff and Permanent Secretary makes explicit reference to the TI-DS GDI which the department has used as a benchmark against which to judge its own performance, and which played a part in them achieving a top score in 2015.

Furthermore, TI-DS and the GDI feature in the United Kingdom Anti-Corruption Strategy 2017–2022: Year 2 Update.[20] Under one of the goals (enhanced action to reduce corruption in fragile and conflicted affected states), the report highlights the UK government's funding of the GDI as evidence as to how they are 'promoting greater defence transparency' around the world. The report also names the GDI as a key measurement tool to monitor corruption trends in UK public sectors. It is an indicator that helps 'measure the scale and frequency of corruption related behaviour within key public institutions, which is essential to understand the scale and reach of corruption in the UK'.

MoD Corruption Risk Self-Assessment

In 2013, one of the authors of this chapter initiated a corruption risk assessment process in Bulgaria's MoD. In the course of two months, and with the involvement of the senior leadership, the following steps were taken:

1. Drafting, testing, and revising the methodology and the guidelines;
2. Collecting assessments;
3. Processing the results;
4. Internal and external communication of the findings.

In the first step, the development team identified five areas of corruption risk factors. Testing allowed for more precise definitions and reduced the areas to four:

- Procurement and contracting;
- Personnel management;
- Budgeting and financial management;
- Operations.

[20] *United Kingdom Anti-Corruption Strategy 2017-2022: Year 2 Update* (HM Government, July 20, 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902020/6.6451_Anti-Corruption_Strategy_Year_2_Update.pdf.

A five-degree scale was used to assess likelihood: 'nearly unlikely,' 'rather unlikely,' 'likely,' 'very likely,' and 'almost certain.' A three-degree scale of 'low,' 'medium,' and 'high' was used to evaluate the potential negative consequences of three different types – 'direct financial losses,' 'impact on policy, capabilities, and operations,' and 'impact on the image among society, allies, and partners.'

The Inspector General of the MoD and the Deputy Chief of Defence managed steps two and three. Nearly 50 experts–members of the political cabinet and senior representatives of each MoD agency and directorate and the structures of the armed forces–completed the survey.

Figure 15.2 sets out the procurement-related risks. The assessment identified the following top three risks:

- Sale of defence equipment items at the discretion of an individual defence official or a small group of officials, e.g. in the lack of respective policy guidance (# 10);
- Lack of public information on defence assets designated for sale (# 11);
- Use of intermediaries (middlemen) in defence contracts (# 9).

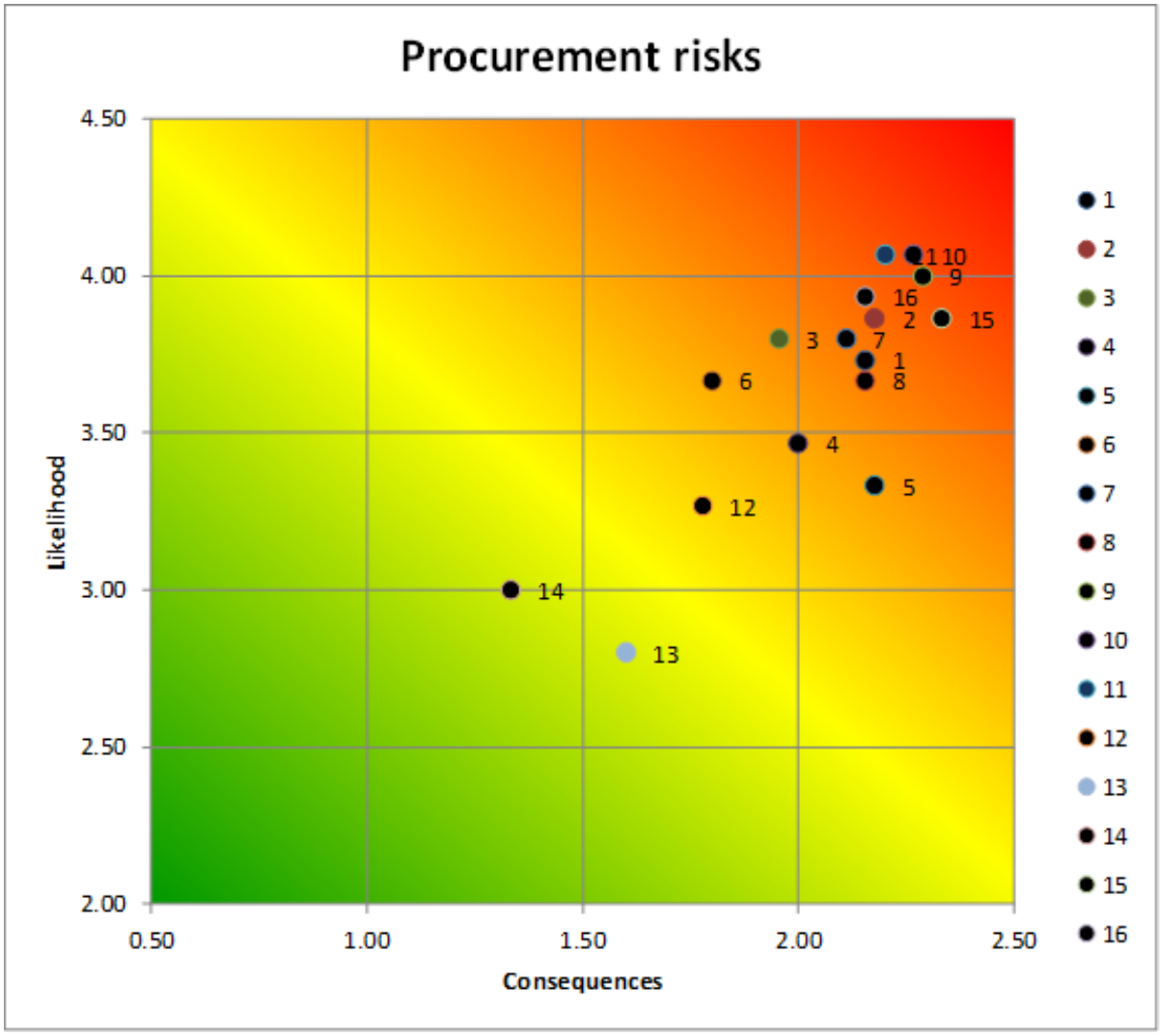


Figure 15.2: Procurement-Related Corruption Risks.

Figure 15.3 presents the corruption risks related to human resource management, where the top two risks are:

- Individual discretion for assignments in international positions, e.g. in the NATO mission (# 5);
- Conflict of interest in assignment and promotion, e.g. assigning relatives to lucrative positions (# 6).

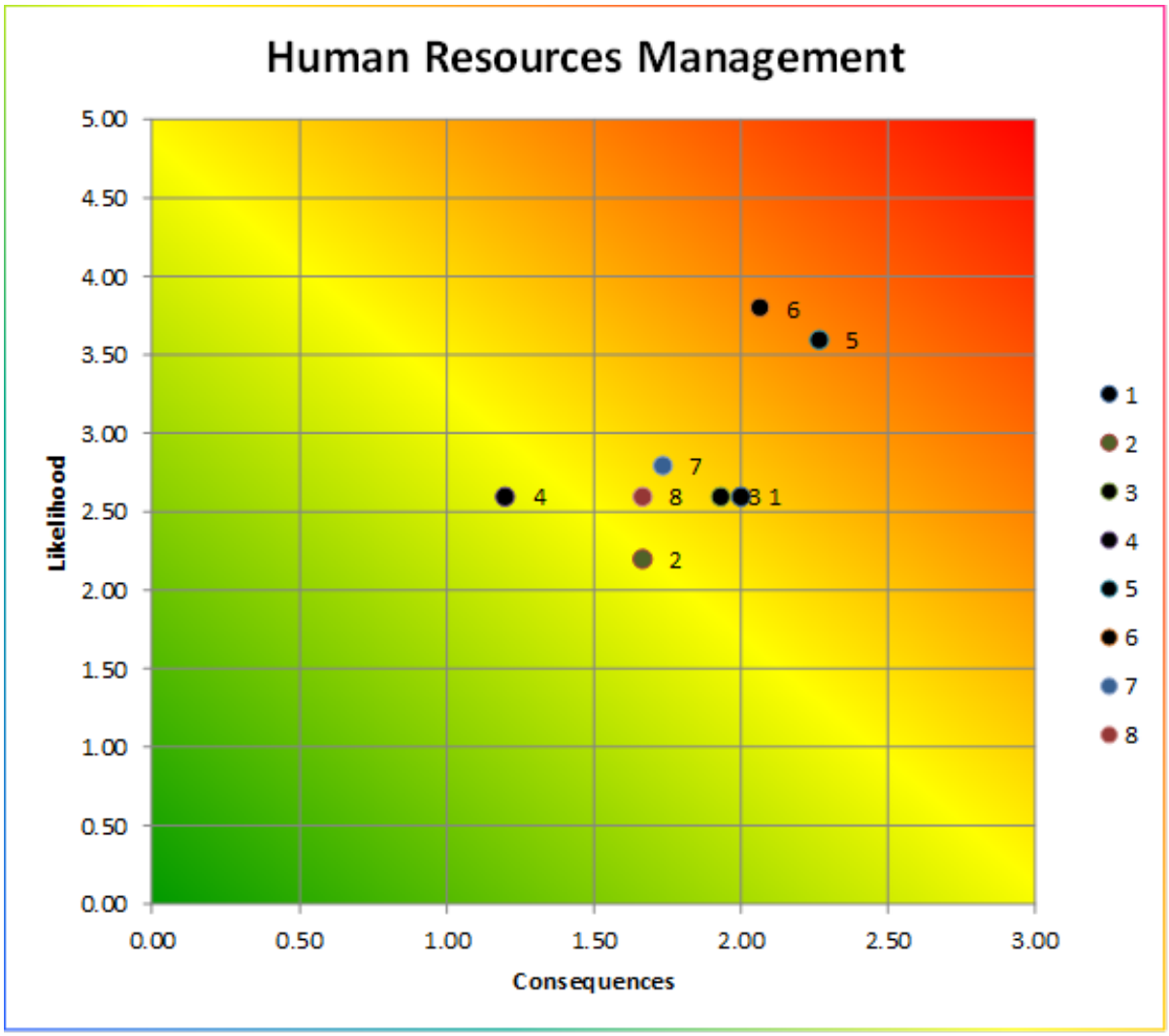


Figure 15.3: Corruption Risks Related to Personnel Management.

Senior leaders communicated the findings and integrity building plans throughout defence organizations. The results were published on the MoD website and picked up by the media, thus raising the societal interest in the problem, as well as in potential solutions. Consequently, the findings informed the discussions in the Anti-corruption Council, chaired by a deputy minister of defence, on relevant risk reduction measures.

Conclusion

The assessment of corruption risks is an important step in developing a building integrity policy tailored to the local context. As the examples of procurement and human resource management risks suggest, the highest risks might differ from those most often discussed in international fora. Hence, reducing the overall corruption risk in a defence organization effectively requires prioritizing measures aimed at mitigating organization-specific high corruption risks. This chapter presented the key concepts, various approaches, and examples of corruption risk assessment and mapping. It emphasized the importance of careful design in the assessment framework, scales, and questionnaires and the preliminary testing and validation. The chapter also pointed to some potential caveats, e.g. the selection of experts conducting the assessment. The presented methods, directly or in some combination, can be applied more broadly and serve as a basis of a risk management policy.[21]

To fully integrate integrity building in mainstream organizational activities, the assessment of corruption risks needs to become part of the overall risk assessment and the mitigation measures to be included in the

[21] See also International Organization of Standardization, *ISO 37001: Anti-bribery Management Systems*.

organizational risk management system. This requires leadership and means continuously integrating, designing, implementing, evaluating and improving risk management across the organization.[22] The following chapter provides guidelines on how this can be implemented in practice.

[22] International Organization for Standardization, *ISO 31000*.

16.Building Integrity Programmes

Prof. Todor Tagarev

Once a defence ministry, a military formation or another security sector organization is aware of the need to enhance integrity and reduce corruption risks, it needs to organize its efforts systematically. A building integrity (BI) programme or roadmap typically serves that purpose. To guarantee sustainable effects, any BI efforts need to become an integral part of the evolving institutional norms and the practice of good governance and effective defence management.

This chapter examines the programme-based approach to integrity building as an important tool using institutional resources efficiently to reduce corruption risks in a defence or security sector organization. Alternative terms may be applied to designate this approach, i.e. using the terms 'roadmap' or 'plan' instead of 'programme.' The decision on using a particular term will be context specific and welcome, as long as BI activities are incorporated as an integral part of institutional management processes. The first section of this chapter presents the principles of good governance and management most relevant to integrity building. Section 2 provides guidance on elaborating a BI programme, while section 3 puts forward good practices for the implementation of such a programme.

1. Principles of Good Governance and Effective Management

To achieve the intended results, integrity building efforts, just like any other institutional activity, need to adhere to tried and tested principles of governance and management.

Authors and some international institutions define the principles of good governance in various ways, depending on the specific area of application, the implementing actor and the supported initiative. For example, the United Nations Economic and Social Commission for Asia and the Pacific has defined eight principles, or characteristics, of good governance in a brochure aiming to support the governance of urban areas.[1] The Council of Europe has provided guidance to local authorities on the '12 Principles of Good Democratic Governance.'[2] The UK's Good Governance Institute defines 'ten principal themes' covering 'the most fundamental and important elements' of organizational governance.[3] All these guidelines emphasize transparency and accountability, ethical behaviour and integrity, as well as effectiveness. Some of the guidelines also point to the clear definition of roles and responsibilities, providing opportunities for: the participation of various stakeholders; leadership; careful and responsible protection and management of organizational assets; reputation and long-term functioning; compliance with standards and targets; comparing performance against best practice; provision of the requisite competencies and capacity; and human rights.

Studies focused on defence reform and integrity building add to these principles: the separation of powers between military and other security sector organizations and the civilian oversight of the armed forces; internal checks and balances; and evidence-based policy-making.[4]

All these governance considerations, discussed under the rubrics of 'principles,' 'basics,' and 'fundamental elements,' are valid for the design and the implementation of BI programmes. Yet, on the other hand, they are not always based on systematic studies. Sometimes they lack a sufficiently clear scope, and they often mix

[1] United Nations Economic and Social Commission for Asia and the Pacific, "What is Good Governance."
[2] Council of Europe, "12 Principles of Good Democratic Governance" (CoE Centre of Expertise for Good Governance, 2018), https://www.coe.int/en/web/good-governance/12-principles.
[3] Good Governance Institute, "The Basics of Good Governance," May 21, 2021, https://www.good-governance.org.uk/publications/insights/the-basics-of-good-governance.
[4] DCAF – Geneva Centre for Security Sector Governance, "Defence Reform: Applying the Principles of Good Security Sector Governance to Defence," *SSR Backgrounder*, May 2019, https://www.dcaf.ch/defence-reform-applying-principles-good-security-sector-governance-defence; Svein Eriksen and Francisco Cardona, *Criteria for Good Governance in the Defence Sector* (Oslo: Centre for Integrity in the Defence Sector, 2015), https://cids.no/wp-content/uploads/pdf/7215-Critera-for-Good-Governance-in-the-Defence-Sector-k6.pdf.

governance and management matters. In contrast, the International Organization for Standardization (ISO) has published standards elaborating the so-called 'Quality Management Principles' for decades. They form the foundation of the ISO 9000 series of quality management standards and are applicable to public and private, large and small organizations.

The current version[5] elaborates seven quality management principles: customer focus; leadership; engagement of people; process approach; improvement; evidence-based decision making; and relationship management. They are briefly examined below from the perspective of integrity building.

Customer focus

The main focus of management is to meet the requirements of customers and to endeavour to exceed their expectations.

Civilian and military stakeholders in the defence establishment, society at large, and through their representatives in parliaments and specialized organizations, international organizations and peers (like other defence ministries participating in BI) can be seen as the 'customers' of BI programmes. Each customer group has its own expectations. A security or defence organization needs to invest efforts in understanding the requirements of its 'customers' and communicate them throughout the organization, inform the customers of its intentions and plans, report on progress during implementation, and monitor evolving customer expectations. Maintaining transparent relations with the customers may prove invaluable for the sustainability of BI programmes.

Leadership

Leaders at all organizational levels need to establish a common organizational purpose and engage those involved in achieving the organization's objectives. This is necessary in order to align policies, strategies, organizational processes and resources. To that end, leaders are expected to communicate the mission, vision, and the strategy throughout the organization. Their task is to sustain shared values and ethical models and serve as positive examples, establishing a culture of trust and integrity, as well as inspiring and recognizing individual contributions.

The effective and efficient management of integrity building efforts requires the involvement of people at all levels, investing in their competences, and acknowledging their contribution. The implementation of these principles leads to improved motivation, personal initiatives and creativity, enhanced trust and readiness to openly discuss problems, share knowledge, and collaborate. It also encourages the greater representation of women at all levels, including in decision-making positions in line with the UN Security Council Resolution 1325.[6] Women can provide a valuable contribution and often play a lead role in building defence integrity, nationally and internationally.[7]

Process approach

Managing the organization as a coherent set of interrelated processes allows for predictable results with the efficient use of resources. A BI programme can be seen as a set of initiatives to streamline and enhance the transparency of key operational and defence management processes with their objectives and clearly established authority, responsibility and accountability for the management of each process. Further, examining BI activities as components of key processes allows for the identification of information needs and resource constraints, performance indicators and their evaluation, as well as determining process interdependencies and risk management.

---

[5] ISO, *Quality Management Principles*, 2nd edition (Geneva, Switzerland: International Organization for Standardization, 2015), https://www.iso.org/publication/PUB100080.html.

[6] United Nations, Security Council Resolution 1325, S/Res/1325, October 31, 2000, https://www.un.org/womenwatch/osagi/wps/#resolution.

[7] See, for example, *Launch of the Building Integrity Tailored Programme for South Eastern Europe*, Brussels, December 13, 2012, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2012_12/20130516_121213-building_integrity-see.pdf.

Previous chapters in this volume discussed some of the core defence processes of interest in designing a BI programme. With the understanding of corruption risks,[8] leaders need to make sure that the corresponding process is sufficiently streamlined, transparent, and there are no extra loops allowing for the core decision-making logic to be circumvented. 'Transparent' here means not only that essential information is available to all stakeholders, and partially to the public,[9] but also that there is a clear logical, and auditable thread of key decisions, i.e. *process integrity*. For example, an auditable thread of defence acquisition decisions should clearly relate decisions on:

- Defence policy objectives;
- Operational requirements;
- Procurement options and choices;
- Contracting & contract management;
- Rationale for involving national defence industries;
- In-service support;
- Utilization.

Much the same can be said of requirements for the transparency and integrity of the budgeting process. For instance, a comprehensive methodology, developed in a format of cooperation among South-East European countries, emphasized the following considerations in assessing the integrity of the budget planning and financial management process:

- The budgeting is based on a rigorous and reliable forecasting of budget and fiscal constraints in a comprehensive macroeconomic framework. The underlying assumptions are clearly documented;
- The defence programmes' costs are estimated by a comprehensive and consistent set of cost factors;
- The accounting practice is consistent, with well documented changes in accounting policy;
- Programme and budget alternatives are identified and documented; decisions to transition from one alternative to another are also documented;
- Records of plans, implementation results and assessments are readily available and easy to compare;
- Accounting reports are audited in a timely and rigorous manner.[10]

Improvement

Successful organizations continuously improve to reflect the changing environment and to exploit emerging opportunities. The link between organizational management and BI programming is twofold. First, the evolving normative, technological, personnel, and organizational conditions need to be reflected in the BI programme. Second, a well-designed and successfully implemented BI programme would ideally have a substantial impact on improving organizational performance and the standing of the armed forces in the public perceptions and attitudes.

A culture of continuous change enhances the organizational capacity to anticipate and quickly react to emerging risks and opportunities; it also facilitates innovation. The implementation of this principle will monitor and review requirements, results, and performance and adapt the BI programme accordingly.

Evidence-based decision making

Decision-making on the basis of data and evidence is more likely to deliver the desired results. The systematic collection of reliable data helps to reduce uncertainty as well as helping to design and evaluate potential courses of action. It increases confidence in making, reviewing and, when necessary, changing earlier decisions.

[8] See the previous chapter in this volume.

[9] Understanding the need for balancing openness and transparency, on one hand, and the protection of the legitimate security concerns on the other. See, for example, OECD and the European Union, "Defence Procurement," Brief 23, Support for Improvement of Governance and Management (SIGMA), 2011, https://www.sigmaweb.org/publications/Public-Procurement-Policy-Brief-23-200117.pdf.

[10] For details see Todor Tagarev, "A Means of Comparing Military Budgeting Processes in South East Europe," *Information & Security: An International Journal* 11 (2003): 95-135, http://dx.doi.org/10.11610/isij.1105.

In the implementation of this principle, planners need to determine in advance how results and performance will be measured and how to define the key indicators to be used for demonstrating progress. Further, people need to be trained to collect and analyse data using appropriate methods. Finally, such data and evidence should be made available to all relevant stakeholders. Ultimately, the accumulation of reliable data may provide for the systematic use of data analytics to improve decisions, for example in the defence procurement process and policy-making.[11]

The gathering of information on corruption risks coming from case studies, perceptions, and expert assessments, was discussed in the preceding chapter. This is only one evidence type essential for the design of BI programmes. Other types of data are discussed in the next section.

Relationship management

Various parties have an interest in the design of a BI programme and may influence its implementation. Success in this endeavour is more likely and can be sustained when the organization invests in managing the relationships with all interested parties. Relationship management will facilitate the common understanding of the goals of stakeholders and their values. It will also enhance organizational performance through the recognition of constraints and a coordinated and timely response to emerging opportunities.

In the implementation of this principle, BI leaders are advised to balance short-term benefits and long-term considerations when it comes to creating conditions for the pooling and sharing of information, knowledge, and expertise. Interested parties should also be kept informed on results and performance. In combination, such relationships allow for the identification of opportunities and enhanced collaboration in BI.

2. Building Integrity Programmes

The seven ISO quality management principles briefly presented above set the foundation for developing and implementing a BI programme. The principles provide general guidance, and can be applied in different ways depending on the nature of the organization and the specific challenges it faces.

As set out in Figure 16.1, the design of the BI programme includes determining:

- The scope of integrity building, including organizational roles, activities, resources and results (in the dashed rectangle in Figure 16.1), internal and external stakeholders, communication channels, influence and resources from external sources;
- Guidance and control: defining a vision for the integrity of the organization, BI goals and objectives, overarching norms and the policies the BI programme needs to adhere to (e.g. international norms and conventions such as the UN Convention Against Corruption,[12] relevant national legislation, national and international policies and standards), allocated budget for the implementation of the BI programme;
- Resources and 'suppliers': staff involved in the design and the implementation of the BI programme, facilities, administrative support, computing and communication infrastructure, and the defence organizations that will supply these resources;
- The direct BI results, or 'outputs': the number of documents produced, normative changes initiated or approved, the number of press releases, the training courses developed, the number of people trained, etc.;
- Impact of the BI programme, or 'outcomes': the change of perceptions and attitudes of internal and external stakeholders, enhanced mission effectiveness, the more efficient use of public resources, an increase in defence capabilities as a result of prevented cases of corruption and mismanagement or recovered funds, increased readiness levels, enhanced resilience, etc.;

[11] Ágnes Czibik, Mihály Fazekas, Alfredo Hernandez Sanchez, and Johannes Wachs, State Capture and Defence Procurement in the EU, GTI-R/2020:03 (Budapest: Government Transparency Institute, December 2020), https://www.govtransparency.eu/state-capture-and-defence-procurement-in-the-eu-2/.
[12] United Nations Office on Drugs and Crime, United Nations Convention against Corruption (New York/Vienna: UN Office on Drugs and Crime, 2004), https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf.

- The BI process: one or a set of interrelated processes demonstrating how BI activities will deliver the anticipated results and effects.

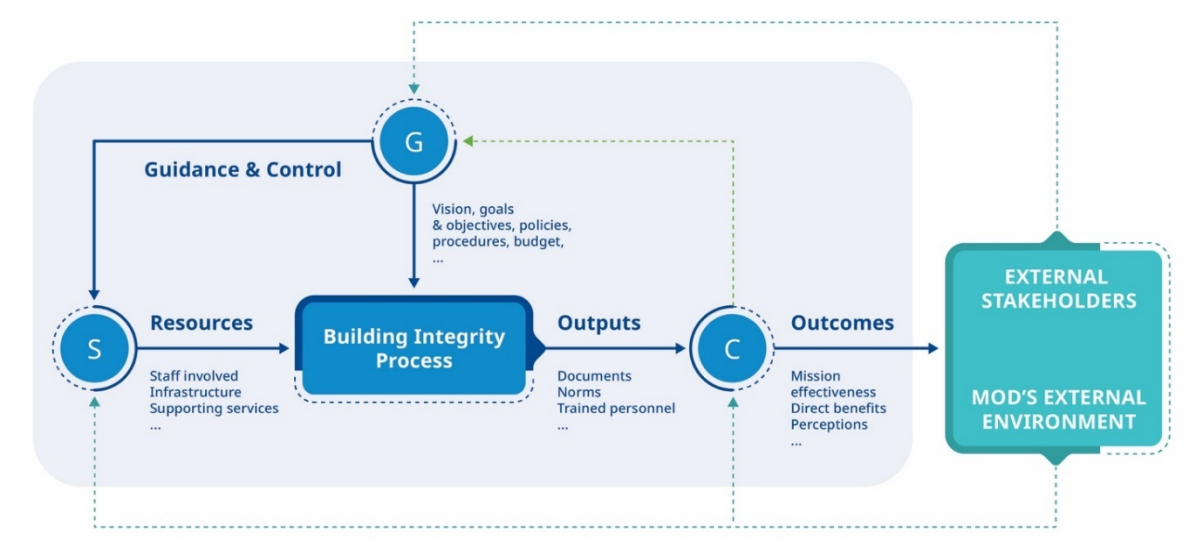


Figure 16.1: BI Process: Guidance, Resources, Outputs and Outcomes.

Box 16.1. Good Practices in BI Design Using the Example of Bosnia and Herzegovina [13]

The Ministry of Defence (MoD) of Bosnia and Herzegovina applied a systemic approach to BI. It aimed to ensure that members of the MoD and Armed Forces behave and institutions operate in a manner that promotes professionalism, transparency, accountability, prevents misconduct and responds properly when wrongdoing occurs. This approach covered relevant organizations, norms, standards of conduct, and procedures. In accordance with the Law of Defence of Bosnia and Herzegovina and the Policy on BI, Risk Reduction and Fight against Corruption in the MoD and AF of Bosnia and Herzegovina, the Inspector General's Office is the primary bearer of coordination of institutional obligations and activities of the MoD and AF related to ethical conduct, BI, and the fight against corruption. The Inspector General is directly subordinate to the MoD.

In support of defence institutional capacity building, the following strategic approach was undertaken:

- Defence Minister's statement on intent, guidance from the top and continuous support to the overall corruption prevention efforts;
- Corruption risk assessment underpinned by the NATO BI Self-Assessment Questionnaire (SAQ) and Peer Review Process, as well as the newly adopted Rulebook on Corruption Risk Assessment of the MoD of Bosnia and Herzegovina;
- Creation of the Integrity Plan and Action Plan for the Fight against Corruption with a pragmatic implementation strategy. The Action Plan includes measures from the Anti-Corruption Strategy of Bosnia and Herzegovina, recommendations from the NATO BI SAQ and Peer Review report, actions from the NATO BI Partnership Goal, audit findings and actions identified by functional divisions of the MoD and the Joint Staff;
- Coordination of the implementation of the Action Plan by the Inspector General. The authority for implementation at the operational and tactical level is delegated to inspectors and ethics officers. This allows unity of effort and regular communication of BI results and achievements, both internally and externally;

[13] This text is provided by BG Enes Husejnovic, Inspector General of the Armed Forces of Bosnia and Herzegovina (after light editing by the chapter's author.).

- The regular work of the MoD Board for BI and the Expert Group for implementation of the policy is essential, since they have the mandate to oversee, control implementation and adjust the policy;
- The Inspector General's Office has a degree of independence with the jurisdiction to: investigate allegations of unethical, unprofessional or illegal conduct, assist members of the armed forces in protecting their rights, implement awareness training on corruption risks, and manage strategic and systemic approach to BI implementation;
- The transparency of defence budgeting, procurement, anti-corruption plans, investigation results and major strategic defence activities has been significantly promoted;
- The MoD has focused the cooperation with NATO, OSCE, TI, UNDP and bilateral support by the United States, Norway and the United Kingdom on integrity and corruption prevention.

The institutional work of the Inspector General's Office and the overall defence sector on BI and corruption prevention ensures proper checks and balances. This includes oversight by the Parliamentary Joint Commission for Defence and Security, cooperation with the Parliamentary Military Commissioner, as well as the national Agency for Prevention of Corruption and Coordination of the Fight against Corruption, and information sharing with the Audit Office of Bosnia and Herzegovina, the Office of the Ombudsman for Human Rights, the Prosecution Office and the State Investigation and Protection Agency.

Designing measures and indicators, and deciding which ones to prioritize, is particularly challenging. A management tool known as a 'Balanced Scorecard' may assist programme designers in defining and structuring measures of results and performance. The Balanced Scorecard was initially developed by Robert S. Kaplan and David P. Norton as a tool to translate strategy into a set of actions with measurable impact accounting for companies' tangible and intangible assets.[14] Kaplan and Norton recommended that companies structure and present organizational objectives, measures of results and performance, targets, and supporting initiatives from four main perspectives:

1. Financial perspective, demonstrating the value to shareholders, including indicators of profitability, market share, etc.;
2. Customer perspective, showing the value of organizational products and services and including indicators of customer satisfaction, e.g. on-time delivery, and sustaining the customer base, as well as indicators of social responsibility;
3. Internal business process perspective, demonstrating how efficient the internal operations are;
4. Learning and growth perspective, showing organizational sustainability and capacity to improve.

Although the tool has been developed with a business focus, it has been applied widely in studies of the management of not-for-profit organizations, including public administrative entities. Various authors have suggested some adaptation of the four perspectives, e.g. de-emphasising the fiscal perspective by moving it from the top position in the traditional visualization provided by Kaplan and Norton and/or suggesting less business-oriented titles for some of the four perspectives.[15] One such example is presented in Figure 16.2. Yet, the structuring remains the same, and the main difference is in the formulation of objectives and measures, in particular for the financial perspective.

[14] Robert S. Kaplan and David P. Norton, *The Balanced Scorecard: Translating Strategy into Action* (Boston, MA: Harvard Business School Press, 1996), https://doi.org/10.1016/S0024-6301(97)80925-9. See also Robert S. Kaplan, "Conceptual Foundations of the Balanced Scorecard," Working Paper 10-074, Harvard Business School, Harvard University, 2010, https://www.hbs.edu/ris/Publication%20Files/10-074_0bf3c151-f82b-4592-b885-cdde7f5d97a6.pdf.

[15] See, for example, Paul R. Niven, *Balanced Scorecard: Step by Step for Governments and Nonprofit Agencies*, 2nd ed. (New York: John Wiley, 2010); Aleksey Savkin, "Example of Nonprofit Balanced Scorecard with 14 KPIs," BSC Designer, June 4, 2010, https://bscdesigner.com/nonprofit-scorecard.htm.



Figure 16.2: A Balanced Scorecard Template for Public Organizations.

Researchers have suggested that the Balanced Scorecard approach may enhance governmental counter-corruption initiatives. For example, El Nashar proposed to use a balanced scorecard in the governmental reporting system of Egypt and as an 'effective tool for external performance reporting … [and] strong incentive for external accountability.'[16] The author applies four perspectives – Financial Sustainability, Internal Process, Stakeholders, Learning and Growth – and for each one suggests a set of strategic objectives and measures of performance. Table 16.1 provides, as an example, the respective definitions for the 'Stakeholders' perspective.

Table 16.1. Strategic objectives and performance measures – Stakeholders perspective

Strategic objectives	***Performance measures***
Promote the government's image	• International ranking • Reputation weight • Citizens evaluation
Satisfy the governmental Oversight board	• Tackling unemployment • Government performance rate • Government growing rate
Governments official loyalty	• Officials leaving work
Increases quality of services	• Quality assessments
Encourage partnerships with related governments	• Joint projects and activities

[16] Tamer A. El Nashar, "Governmental Balanced Scorecard to Tackle Corruption in the Governmental Sector," SSRN Research Papers, December 2020, p. 3, http://dx.doi.org/10.2139/ssrn.3751431.

A study on using the Balanced Scorecard (BSC) to reduce 'financial and administrative corruption' in the Iraqi Government, published in 2022,[17] identifies the 'full adherence to the application of international and local professional auditing standards' as one of the main ingredients of the BSC. The authors claim that there is a significant correlation between the BSC and the professional performance of accountants and auditors, as well as between the BSC and the fight against financial and administrative corruption.[18] Finally, they recommend the use of the BSC as 'an important tool in addressing the manifestations of financial and administrative corruption and limiting its causes.'[19]

Another non-defence example comes from the Philippines. The mayor of a city, previously plagued by corruption and in need of radical transformation, decided to implement a performance governance system employing a balanced scorecard.[20] Importantly, the transformational leader succeeded in overcoming the huge implementation obstacles through empowerment. He identified entrepreneurial governmental employees to drive implementation, used 'experiential learning' to motivate other employees and raise trust and, leading by example, adopted an iterative approach to build and sustain support across the organization.

The use of the balanced scorecard is often accompanied by the creation of a 'strategy map' –a graphic representation of the cause-and-effect connections between strategic objectives.[21] This approach has been implemented by a technical team of the NATO Science and Technology Organization to develop and put forward a new defence performance management framework (see Box 16.2. below).

Box 16.2. Proposed Defence Performance Management Framework

A technical team of the Systems Analysis and Studies (SAS) Panel of NATO's Science and Technology Organization conducted national performance management surveys, a structured literature review, and collected expert opinions and recommendations. On that basis the team drafted a new defence performance management framework and proposed a way for its implementation.[22]
Two concepts underlined the drafting of the framework: 'Strategy maps' and 'Ends-Ways-Means.'[23]
Ends-Ways-Means, in particular, served to organize performance perspectives and potential measures. In terms of outputs and outcomes, the authors identified the following high-level performance categories of interest:

- National interests and defence and security needs;
- Ready force elements;
- Mission outputs and effects;
- International credibility;
- National credibility.

3. Programme Implementation

The sections above presented advanced practices, management standards and examples applicable to the design of BI programmes. Yet ultimately, BI success depends on its effective implementation. As in the design phase,

[17] Saoud Jayed Mashkour Alamry, Hayder Abbas Al-Attar, and Abdulhadi Salman Salih, "The effect of using the Balanced Scorecard (BSC) on reducing the financial and administrative corruption in Iraqi Government Units," *International Journal of Financial, Accounting, and Management* 4, no. 1 (2022): 67-83, https://doi.org/10.35912/ijfam.v4i1.732.
[18] The published results do not provide a description of essential research methods and tools and, hence, do not allow to verify this claim.
[19] Alamry et al., "The effect of using the Balanced Scorecard," p. 81.
[20] Melissa Mahoney and Robert Klitgaard, "Revitalizing Mandaue city: Obstacles in Implementing a Performance Governance System," *Policy Design and Practice* 2, no. 4 (2019): 383-399, https://doi.org/10.1080/25741292.2019.1642072.
[21] Robert S. Kaplan and David P. Norton, *Strategy Maps: Converting Intangible Assets into Tangible Outcomes* (Boston, MA: Harvard Business Review Press, 2004).
[22] Joaquim Soares et al., *Performance Management in Defence Organizations*, STO Technical Report STO-TR-SAS-096-Part-I (Paris: NATO Science and Technology Organization, January 2020).
[23] See, for example, Henry Bartlett, G. Paul Holman, and Timothy E. Somes, "The Art of Strategy and Force Planning," in *Strategy and Force Planning*, th ed. (Newport, R.I.: Naval War College Press, 2004), pp. 17-33.

general good governance and management principles and practices apply to the implementation of BI programmes. That includes: the sustained involvement of the senior leadership; the provision of adequate resources; empowering key contributors at all organizational levels; regular reporting of results; maintaining channels for reporting suspected cases of corruption, etc. This section will briefly outline a few selected implementation activities: progress tracking; communication; risk management; and regular reviews and updates.

Tracking Progress

Progress on the implementation of a BI programme needs to be continuously monitored. The people involved in programme implementation need to be aware, on a weekly or even daily basis, of where they stand in regard to set targets. Key Performance Indicators (KPIs) serve that purpose.

As a rule, KPIs are defined in the design phase. They can be of two main types: leading indicators; and lagging indicators.[24] Both types are needed to track progress. Leading indicators are precursors of future results; lagging indicators show what the organization has already achieved. An example of a leading indicator is the number of articles in the media that report conflicts of interest, suspected cases of corruption or criticize the performance of the defence ministry in its counter-corruption efforts. A respective lagging indicator would be the society's perception index of corruption in the defence sector.

Data and information used to calculate KPIs need to be reliable and verified. Advanced information systems allow for the storage of large amounts of relevant data and visualizing progress, e.g. *via* a 'KPI dashboard.' Such an approach focuses the attention on the most important aspects of BI, searching for improvement opportunities, and a solid analytical basis for decision-making. It will also facilitate evidence-based communication and reporting.

Communication

Honest communication of not only achievements, but also remaining challenges, is essential for sustaining support within and outside the organization for the BI programme. Box 16.3. below presents the key principles of BI communication.

Box 16.3. Communication

Once the BI plan or programme is approved, the handbook for defence practitioners on designing and implementing an *Integrity Action Plan* [25] recommends that it be distributed in writing to all members. It should make clear individual responsibilities for each task and include mechanisms for feedback, adjustments, and updates.

Internal Communication

It is important to keep the wider defence establishment aware of the ongoing efforts with respect to building integrity. Building internal support through an internal strategic communications campaign will prove useful when engaging with the various departments that are highlighted and expected to deliver in the action plan. In addition, it can increase motivation and lets staff know that this is something the leadership, and the defence establishment as a whole, takes seriously.

External Communication

An external-facing communications campaign 'can assist in building support and trust between the public and the defence establishment.' An MoD will be able to establish a reception office and channels for communication with citizens on issues related to corruption and integrity. The messaging to external

[24] Stephen Knack, "Measuring Corruption: A Critique of Indicators in Eastern Europe and Central Asia," *Journal of Public Policy* 27, no. 3 (2007): 255-291, https://doi.org/10.1017/S0143814X07000748.
[25] Bård B. Knudsen et al., *Integrity Action Plan: A Handbook for Practitioners in Defence Establishments* (Oslo: Centre for Integrity in the Defence Sector, 2014), pp. 29-30.

stakeholders needs to be realistic, 'as challenges, delays and an inability to meet established targets could harm the legitimacy and success of building integrity efforts in the eyes of the public.' For example, if a defence ministry decides to establish a reception office and a hotline for corruption signals, it needs to provide resources and authorized personnel to deal with complaints, and thus to meet public expectations.

Risk Management

Risks for the successful implementation of a BI programme and ways to mitigate them need to be considered in the design phase. Risk management is a key implementation function. It includes the monitoring of acknowledged risks; the identification of potential new risks; the development and analysis of mitigation measures; and, when appropriate, the application of selected mitigation measures.

Delays in the adoption of anticipated legislative changes, loss of key personnel, competence gaps, and others may put the implementation of a BI programme at risk. In some cases, the mitigation measures are obvious, e.g. provide training to involved personnel to raise their competences to the required level. Other cases, e.g. lacking legislation, innovative solutions may be needed to alleviate the impact of the respective risks. The leadership of the BI programme is directly involved in risk management. In some cases, risk mitigation may require the discretion of the most senior leaders in the defence establishment.

Review and Updates

Marshal Helmuth von Moltke the Elder, considered one of the most influential military thinkers of the nineteenth century, is credited with stating that 'no plan survives first contact with the enemy.'[26] It is safe to say that BI programmes are usually implemented in environments that are far less uncertain than armed conflicts. Yet, various shifts can make the adherence to initial plans either impossible or inefficient: legal and organizational changes; resource constraints; deviations from planned activities; failure to achieve anticipated interim results; new data; and emerging good practices and opportunities, among others. Therefore, progress in implementation is subject to regular reviews.

In practice, all the components of a BI programme, discussed above, are subject to review and revision. All revisions need to be properly documented, with a clear explanation of the rationale. Any substantial changes in expected results, timelines, and allocated resources would require the sanction of the original approval authority, i.e. senior leaders of the defence establishment. As such they need to be communicated to all key stakeholders.

Conclusion

The design and the implementation of BI programmes do not, in principle, differ significantly from other management activities. There is an abundance of good practices, management standards, and guidelines applicable to BI. This chapter presented selected standards, planning and evaluation tools, such as the Balanced Scorecard, which can be of considerable benefit to defence establishments willing to launch a BI programme or to reassess and enhance their current approach.

However, there are no ready-made solutions. Any BI programme needs to take into account context. That includes, among others, the specifics of the national legislation and justice system, political and institutional arrangements, national and organizational culture,[27] available and accessible knowledge and expertise.

[26] The actual written version is a bit longer: "No plan of operations extends with any certainty beyond the first encounter with the main enemy forces." See "No Plan Survives First Contact with the Enemy," *Quote Investigator*, May 4, 2021, https://quoteinvestigator.com/2021/05/04/no-plan/.

[27] For the role of culture in the related field of defence institution building see, for example, Judith Reid, "Cultural Foundations of Transparent Governments," *Connections: The Quarterly Journal* 16, no. 2 (2017): 81-89, https://doi.org/10.11610/Connections.16.2.05.

The design of the BI programme is an iterative process of drafting and refinement that needs to involve all relevant institutional players. Further, a public announcement of intentions and timelines will give discipline. It will also encourage NGOs/watchdogs to follow the initiative, request information from various stakeholders, and contribute with their views and proposals. Key stakeholders, such as specialized journalists and societal organizations and defence suppliers, may be invited to provide feedback on advanced drafts and, later, on implementation reports. Overall, a carefully designed communication campaign will be of benefit for integrity building.

Finally, BI activities need to become an integral part of performance management in the defence organization. For countries that still lack a system for performance management, the design and implementation of a BI programme based on the principles and concepts outlined above, will provide a substantial contribution to defence institutions' BI goals and good governance in defence more generally.

Case Study: A Values Charter in the Luxembourg Armed Forces

Dr. Erny Gillen and Gen. Steve Thull[1]

The Values Charter of the Luxembourg Armed Forces (LAF) and its associated Military Code of Conduct were developed in 2019 and 2020 through a unique collaborative process under a steering committee of leaders from the Ministry of Defence (MoD), the LAF and an external expert in ethics. In this article, we will describe (1) the innovative concept, (2) the comprehensive and participatory process and (3) the results. For the ease of our readers, each section can be studied separately. Our contribution was commissioned by the MoD.

1. Conceptual Background and an Unprecedented Political Initiative

Values and Identity

Values and virtues are at the core of military commitment. They often invisibly shape the identity and life of soldiers[2] and civilian members of the armed forces. Values and virtues indicate an inner direction giving orientation to people even in wastelands beyond paved roads and traffic lights. Well-trained soldiers can rely on those values, especially in worst-case scenarios. But values and virtues can also become slippery slopes if they are underdetermined and not contextualized.[3] Think about the strong but shallow value of military discipline. For example, in Nazi Germany this value was isolated, absolutist and personified. Thus, soldiers of all ranks were reduced to mere instruments in the hand of the 'Führer'. Out of context and out of conscience, discipline can lead to abominable crimes against humanity, while contextualized and morally embedded discipline contributes to shaping good people and to achieving right objectives in a right way. *Individual values must be linked to and understood as part of a whole system of values.*[4]

Values in Differences

The same values and virtues can have many names, especially in a multilingual, multicultural, or multi-religious country like Luxembourg. Recruits reflect our open society and enter the armed forces not as blank slates, but as young citizens with diverse horizons and value systems, where language, force, violence, or matters of gender may be handled substantially differently. Think about respect as a value. In a male-dominated culture, woman soldiers are looked at differently than in a culture based on equal rights and obligations. The tragic events in Afghanistan, but also the Me-Too movement in North America remind us that the concepts of respect evolve over time and history through cultural shifts and perspectives. To capture the meaning of respect one has to dive deeply into the psyche, history and language of an individual person or collective bodies. *Values are transported in equivocal narratives.*[5]

---

[1] Dr. Erny Gillen coordinated the Flagship Values of the Luxembourg Armed Forces process as ethicist. General Steve Thull is Chief of Defence of the Grand-Duchy of Luxembourg. While this case study is significantly longer than other case studies in this publication, the decision was to, nevertheless, include it as a particularly good example of good practices in the field of building integrity in the defence sector.

[2] In this article we are using 'soldier' as a generic and inclusive term encompassing all uniformed members of the armed forces.

[3] Cf. Shannon E. French, *The Code of the Warrior: Exploring Warrior Values Past and Present*, 2nd ed. (Lanham, MD and New York: Rowman & Littlefield, 2017); Michael Skerker, David Whetham, and Don Carrick, eds., *Military Virtues* (Havant: Howgate, 2019).

[4] 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. Jasutis G., Mikova R. *Comprehensive Toolkit for Defence Ethics: from Principles to Practice*, (Geneva: DCAF - Geneva Center for Security Sector Governance, 2026), https://www.dcaf.ch/toolkit-defence-ethics-principles-practice.

[5] Cf. Paul Ricœur, *Soi-même comme un autre* (Paris: Seuil, 1990); Paul Ricœur, Temps et récit (Paris: Seuil, 1983-85); Dietmar Mieth, *Moral und Erfahrung* (Fribourg: Herder, 1998-99).

Values and Rules

Commonly lived values and virtues interact with norms and rules, especially in hierarchically organized structures like the armed forces. As one and the same value – when understood in a different context, can shape contradictory behaviour, it is important to draw common red lines in an unequivocal language. This is the *raison d'être* of military codes of conduct applying to all soldiers. Think about a proper salute. As part of the drill and the daily routines, this acquired automatism can express honour, respect, and loyalty. But it can also communicate disdain, and degradation if not performed or reciprocated properly. Thus, a culture of proper saluting fosters mutual integrity and professionalism. Rules and norms express and protect values. The proper interaction between values and rules is an ethical challenge in all pedagogical processes driven by values, but they are paramount for armed forces. *Values come first and provide meaning for rules.*

Values and Ethics

Specialists trained in behavioural sciences know that people buy into values when reaching out for new devices or working environments. Advertising for products, services or positions is carefully designed to nudge behaviour through values. In that context values are either strong motivational drivers or sources for serious frustration and disappointment. In that sense, values are commonly shared inner moral grounds, leading and explaining people's behaviour and actions. Where values are more used as a facade than an expression of an authentic culture, double standards make their way into daily interaction. *In each group values must be an honest expression of an ideal reality strived for by all involved.*

Values and Armed Forces

Given this general understanding of the role of values and norms, the Luxembourg Armed Forces were invited and supported by the MoD, François Bausch (Green Party) to initiate an open and ethically based process for identifying, codifying and implementing a set of flagship values. This truly unprecedented political initiative was triggered by a genuine interest in the role and function of the LAF in and for Luxembourg society. Unlike in other countries, no public ethical failures or incidents kicked off the process. This specificity has shaped a unique, comprehensive, and participatory process under the lead of two successive Chiefs of Defence (CHOD) with their staff and an independent expert in ethics.

2. A Multifaceted Process

We are now describing the process of the two-year-long project run in 2019 and 2020 under the title '*Flagship Values of the Luxembourg Armed Forces'.* The results laid out in the third part of this contribution are a Values Charter with a Commentary, a Values Table, and a Code of Conduct, all publicly accessible on the armed forces' official website: www.armee.lu[6].

How it Began

As we are looking back to the early days of this process, it becomes even more obvious how important it is to start such an endeavour without fear and pressure. The open-minded political interest in the armed forces themselves fostered a serene climate in a small country where soldiers are deployed at home to help the population cope with natural disasters or public health issues and to be present at solemn national events. In the international arena, the LAF participate in international missions by joining UN, EU or NATO mandates under the command of other nations' armed forces.[7] The LAF, with around a thousand servicemen and women, count

[6] Direction de la défense, Government of Luxembourg, «Engagement, droiture et fiabilité: présentation de la première charte des valeurs de l'Armée luxembourgeoise, » October 15, 2020, https://www.armee.lu/actualites/2020/engagement-droiture-et-fiabilite-presentation-de-la-premiere-charte-des-valeurs-de-l-armee-luxembourgeoise.

[7] E.g. the LAF participate in the Enhanced Force Presence Mission in Lithuania: North Atlantic Treaty Organization (NATO), "NATO's enhanced Forward Presence Battlegroup Lithuania marks its 4th rotation," Supreme Headquarters Allied Powers Europe (SHAPE),

soldiers and civilians from more than eight different nationalities, many of whom have a migrant background.[8] Public trust in the LAF is high and there are very few political discussions today about its *raison d'être* or its participation in operations.

Established after the Second World War and a period of brutally ignored neutrality, the LAF were built up on the British model. Today, its officers and NCOs are trained in the military institutions of Belgium, France, Germany, the United Kingdom, and the United States, as it is the case for most medical doctors, lawyers and academics in our country. Luxembourg has absorbed many local and foreign cultural and educational influences. This has led to specific ways of living (*modi vivendi*) that tend to remain informal rather than being codified or written down. From a sociological point of view, it was then not surprising that the LAF did not possess a written values charter, even though some preliminary work had started before the Minister launched this initiative.

By proposing an internally recognized and experienced ethicist to facilitate the Flagship Values Project, the Minister created right from the start a climate of professionalism, opportunities, openness, and trust. Once the design of the project was accepted by the military leadership, a steering committee created by the CHOD with his delegates and members of the Directorate of Defence was put in place. The Steering Committee had the contractual authority to adapt the project plan and timing within the agreed boundaries. It met five times for formal meetings and was consulted many more times *via* mail to address specific questions. Together with the internal LAF working group the Steering Committee was a guarantee for a smooth and fair process. The internal working group was led by the Command Senior Non-Commissioned Officers and facilitated, together with the communication department, all contacts with soldiers and civilians as well as the logistics for meetings and conferences.

In addition, two events proved important for a good start to the project: a connection with the international community of military ethicists and a visit to a centre dealing with values and integrity. Becoming a member of The International Society for Military Ethics in Europe[9] and taking part in its annual conference in Vienna in May 2019 was useful for meeting experts and to start networking. This was followed by a joint visit with the Command Senior Non-Commissioned Officers and the newly appointed official in charge, to the Central Organisation Integrity Defence (COID)[10] of the Dutch Ministry of Defence in Utrecht. Their shared experiences, tangible results, motivation, ambitions, and support served as a supplementary booster to go ahead with the intended bottom-up process approach. Derek Suchard, furthermore, fostered contacts and meetings with the NATO Building Integrity Programme. Thanks to that international and professional network of military ethics, the LAF were comforted in their task to identify, codify, and implement a set of core values.

Quality Interviews and Their Compilation in Value Clusters

In total, 56 people took part in interview sessions of around one hour each. The interviews followed a questionnaire guiding interviewees to express themselves as much as possible about their leading motivation when entering the LAF and their present motivation to continue their commitment. Interviewees were invited to reflect about any shifts in their motivations and to reflect about endogenous and exogenous, general or specific situations as reasons for those changes. Based on their narratives the interviewer mirrored explicitly and implicitly mentioned values and raised further questions about conflicting values as well as language

September 13, 2018, https://shape.nato.int/efp/latest-news/natos-enhanced-forward-presence-battlegroup-lithuania-marks-its-4th-rotation (accessed February 23, 2026); European External Action Service, *EUTM Mali: European Union Training Mission in Mali - Military Mission*, November 30, 2020, https://www.eeas.europa.eu/eutm-mali/eutm-mali-european-union-training-mission-mali-military-mission_und_en (accessed February 23, 2026); and UN Peacekeeping , "MINUSMA," https://minusma.unmissions.org/en (accessed February 23, 2026).

8 Direction de la défense, Government of Luxembourg, «Engagement, droiture et fiabilité: présentation de la première charte des valeurs de l'Armée luxembourgeoise.»

9 EuroISME, https://www.euroisme.eu/index.php/en/ (accessed February 23, 2026).

10 Ministerie van Defensie, https://www.defensie.nl (accessed February 23, 2026).

preferences. The voluntary interviewees were also invited to position themselves with their present convictions about values in their respective groups and the LAF in general. The interviews took place in complete confidentiality and the notes were destroyed at the end of the project.

Interview candidates were invited and selected from all ranks, age and gender categories to provide a balanced insight into the values currently lived, perceived and expected within oneself and within the others. With one exception, all interviews took place in Luxembourgish. Luxembourgish allows speakers to choose between native, French-derived, or German-derived words to express the same idea, and the interviews were conducted in that language. When most interviews were conducted and patterns became visible, lists of word families were created out of the three Luxembourgish language sensibilities. Word families were counted and weighted, and value families were tentatively merged in five-word clouds reflecting the weightings both in terms of language and values. These word clouds were added into the last series of interviews beginning in 2020 when the youngest interviewees were asked in additional sessions, individually and in small groups, to express their understanding of the different value families and their preferences.

By the end of February 2020 three super values with their synonyms and variants could be presented to the Steering Committee: engagement, righteousness, and reliability.[11] They were by far the most mentioned and generally understood values. Through the in-depth interviews it had also become clear that those flagship values needed to be translated differently into four specific dimensions in military life and work: the individual soldiers; the group they are part of; the task they are assigned to; and the general mission they serve.

Building and Validating a Values' Table

Through expert discussions on ethics with key actors within the LAF, the MoD, and institutions specialized in military ethics from Belgium,[12] France,[13] Germany,[14] Norway,[15] the Netherlands,[16] and Switzerland,[17] a first Values Table was developed. It aimed at bringing a systematic and pedagogical order into the three core values expressed through the four dimensions (see illustration 2).

1. Which sub-values are represented under the super-values reliability, righteousness, and engagement?
2. How do those sub-values interact within the respective personal, group, task, and mission dimension?

The table quickly became a core instrument in expert and feedback discussions. But did it still capture and represent the results of the 56 interviews? To verify that, the table in which values and their wordings were changed and shifted was presented to four focus groups with 37 of the 56 interviewees in the military centre in Diekirch. Each workshop had soldiers and civilians from different ranks, age and gender groups. An open and fair setting was created through a virtual tool allowing everyone to express their opinion anonymously, simultaneously, and visibly on a screen.[18] Younger participants were invited to take the floor first at each round. The aim was twofold. One, to check whether interviewees could understand and accept this result as part of

[11] In the original French text those three flagship values read: 'engagement, droiture et fiabilité.' In German they translate 'Engagement, Rechtschaffenheit und Zuverlässigkeit.'

[12] Royal Military Academy, Brussels, https://www.rma.ac.be/en (accessed February 23, 2026).

[13] Académie militaire de Saint-Cyr Coëtquidan, https://www.st-cyr.terre.defense.gouv.fr (accessed February 23, 2026).

[14] Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr, https://www.bundeswehr.de/de/organisation/weitere-bmvg-dienststellen/zentrum-militaergeschichte-sozialwissenschaften and 'Zebis' https://www.zebis.eu/home/ (accessed February 23, 2026).

[15] Centre for Integrity in the Defence Sector, Norway, https://www.cids.no (accessed February 23, 2026).

[16] Centrale Organisatie Integriteit Defensie, https://www.defensie.nl (accessed February 23, 2026).

[17] Militärakademie an der ETH Zürich, https://berufsoffizier.ethz.ch/partner.html (accessed February 23, 2026).

[18] 'Mentimeter,' https://www.mentimeter.com (accessed February 23, 2026).

their own contributions and a future value-based military environment. Two, to validate the table of values as it had evolved many times over time through this process of validation. The outcome was stunning. Each workshop was creative and contributed to defining the final table as it was later accepted by the military leadership during the Steering Committee meeting.

Drafting and Validating the Values' Charter and its Commentary

In mid-April 2020, the project coordinator presented a first draft for a Values Charter of the LAF. (1) In an introductory paragraph, the international and institutional context in which the LAF operates as the military branch of the Grand-Duchy of Luxembourg was described. (2) In the next paragraph the military and civilian members of the LAF accepted that mandate and the given authority within that specific international and national framework by saying 'we'. (3) From that point onwards the LAF and their members are the subjects speaking. They acknowledge the process through which the values were identified and codified in the Charter. They describe what those values mean to themselves, their mission, and the citizens they serve. (4) Then the draft expressed the three flagship values each in a synthetic sentence articulating their four sub-values. (5) In a final paragraph they collectively commit to the Values Charter.

Again, eight major drafts written in French, and with many variants, were discussed internally in Luxembourg and in peer reviews with the seven partner institutions specializing in military ethics. The final draft was presented by the end of June 2020 to the Steering Committee, and during its meeting, the military leadership accepted the version to be presented to the Minister of Defence who had initiated the process. Once the Minister of Defence had accepted the final draft, the last three stages in the process could be prepared. Since the end of February 2020, the successor of the outgoing CHOD has been designated by the Minister of Defence. From that moment onwards, the Ministry got involved in drafting the Charter and the next steps. The open and result-oriented transition between the successive CHODs was a key success factor one should not underestimate.

After having presented and discussed the many drafts and the final text of the Values Charter at length it appeared that a Commentary to its succinct text would be beneficial for internal and external use. A draft written in French was developed by the project coordinator and reviewed by the internal working group and the Steering Committee. Once the text was fixed and agreed upon, the decision was taken to produce an A4 formatted brochure / leaflet including the Values Charter, the Commentary, and the Values Table in French. To make this set available in Luxembourgish, which serves for daily communication, it was decided to translate all three documents into Luxembourgish. This was done by the coordinator and reviewed by the communication department and internal working group before the final text was approved through the Steering Committee by the military leadership.

This translation encouraged the internal working group also to prepare two working translations into English and German with the intention of facilitating any international communication in this sensitive domain. Whereas the French version of the brochure serves as the original text, the different translations showcase how difficult it is to effectively communicate about ethical concepts, values and rules in diverse languages and cultures.

Preparing and Organizing an International Seminar Around the Values Charter

In his 2019 Report on *The OSCE Approach to Security Sector Governance and Reform (SSG/R)* the Secretary General invites participating states to 'actively engage in constructive dialogue to build a common understanding of SSG/R' and to support through these efforts 'the implementation of 2030 Agenda for Sustainable Development and the UN's "Sustainable Peace" agenda.'[19] Our experience in Luxembourg certainly confirms that such international efforts are highly beneficial. At all times, our national endeavour could count on expert advice from other military ethicists knowledgeable about the specificity of our country.

[19] Organization for Security and Co-operation in Europe (OSCE), *The OSCE Approach to Security Sector Governance and Reform (SSG/R): Report by the Secretary General* (Vienna: OSCE, March 20, 2019), https://www.osce.org/secretary-general/414725.

Before the COVID-19 pandemic hit us, an international workshop around the Values Charter was foreseen for May 2020 but it had to be cancelled. Thus, the peer reviews had to be conducted through videoconferencing with the experts of the seven partner institutions. After the endorsement of the Values Charter in September 2020, it became clear that any international military workshop would only make sense if the purpose of an in-person meeting were redefined. Steve Thull, co-author of this article and Luxembourg CHOD argued for a practical workshop focused on the implementation of values in partner armed forces. The seven partner institutions and their experts agreed to convene for that purpose in Luxembourg and to share and discuss their experiences and educational tools. The international Workshop took place on 12 and 13 October 2020 at the Military Centre Grand-Duke Jean with some international experts present and some connected *via* videoconference.

This academically and practically designed workshop brought 67 local participants together with international experts to discuss best practices for educating soldiers and civilians in a value-based environment. After an introduction about the necessity of a value driven corporate culture, the members of the LAF split into small groups to intensively exchange implementation strategies, tools and methods with the experts. The Minister of Defence hosted a dinner at the military centre and entered into vivid dialogues with the international guests. In his address to the audience, the Minister emphasized how much he supports the chosen approach and values the results generated through the collaborative approach. His encouragement and the ambition of the CHOD to go further gave this workshop more a note of a starting point than a ceremonial thanksgiving. Further support from the MoD was shown through the active presence and contributions of several officials during the two days.

At the end of the international workshop, the CHOD met with the Luxembourgish participants to draw conclusions. The major outcome was the creation of an internal group tasked to draft a Military Code of Conduct by the end of the year 2020.

Internal and Public Presentations of the Values Charter

Days before the international workshop, two internal sessions for all members of the LAF were organized to inform them about the process and the contents of the Values Charter. A few days later the Charter was publicly presented by the Minister of Defence, the CHOD, and the external expert. During the media conference, the CHOD also announced his resolution to enforce a specific Military Code of Conduct reflecting the Values Charter for the daily routine, life, and work of all soldiers.

The Charter states explicitly that it also aims at supporting 'the trust citizens naturally place in Luxembourg's armed forces'. This is an important part of the process, as you can only measure someone's values when you know them. The media conference was widely covered and well received.

Drafting and Putting into Force a Value-Based Code of Conduct

Before drafting the requested Code of Conduct, a group of military personnel representing the four corps met under the lead of the Head of Resources and Employment Division within the General Staff, LtCol Alain Schoeben, to study existing codes of conduct from other armed forces. The coordinator of the flagship values project assisted in this work by facilitating the exchanges and helping to extract self-commitments from the Values Charter. In only three sessions, with a lot of drafting work done in between, eight self-commitments were formulated. They were presented just in time to the CHOD who approved them with the acceptance of the Steering Committee in its final version. Thus, the CHOD put them into force and presented them publicly before Christmas to his troops and the press.

Each sentence of this Code of Conduct articulates *several* values with a sentence of self-commitment. Thus, it becomes clear that values must be balanced and that they need a concrete person taking responsibility and attempting to live up to that norm. Let's take the second rule laid out in the Code of Conduct as an example: 'I fulfil my mission with determination, responsibility and initiative, and once done I look after myself!' This

example shows what is expected from soldiers: they fulfil their mission as responsible, proactive, and determined subjects who only look after themselves once the mission is completed. Each soldier promising to live up to that standard will feel the ethical challenge and choices they are entrusted to make. Each sentence in this Code of Conduct articulates that appeal and hands it over to the person saying just one word: 'I'! In this sense the Code of Conduct translates the Values Charter into different situations and addresses soldiers' consciences in their daily work as comrades.

3. Results and Learning

Ethical Thinking Fosters Responsibility

People and institutions must take care of their ethos through ethical reflection and reviews. Moral norms do not fall from heaven and they are not carved in stone. It is the duty of every generation to make sure that it masters its unique challenges on the background of its traditions and within the framework of universally forged and accepted moral principles. Those principles must be applied in concrete life and they demand moral integrity and creativity. As open concepts, principles and values must be integrated into meaningful narratives which combine personal experiences with personal ambitions, thus opening hearts and minds to go ahead.

Values Charter of the Luxembourg Armed Forces (LAF)

The Values Charter is certainly the most tangible result of a transparent process within an ethical framework. Its elaboration was designed as a practical learning field and included many actors. Every word and every sentence were weighed by different people and looked at from different perspectives. It is truly the result of a professionally moderated and participatory process. It authentically expresses today's narrative of the LAF which will continue to evolve in our complex world where the borders of peace and warfare have become moving grounds again. In some years it will be reviewed by new people and developed further based on new experiences and learnings. Texts like the Charter are snapshots encapsulating situational moments in a bigger picture.

Values Charter
of the Luxembourg Armed Forces

The Grand Duchy of Luxembourg, a founding member of the United Nations, the North Atlantic Treaty Organization and the European Union, is deeply committed to the development of an open international culture based on the rule of law, peace and universal values. Within this framework, the Luxembourg Armed Forces, Military Corps within the Public Administration, is entrusted with the mission of assisting and protecting the population and the institutions of the Luxembourg State, defending the freedom of the Nation and contributing in solidarity with its partners to international peace.

Thus, we, military and civilian members of the Armed Forces have been given the authority and means to exercise our mandate to the best knowledge and belief within the framework of international law, the Constitution, the laws and regulations of the country and in accordance with our oaths of allegiance.
This Charter, developed through a collaborative process**,** sets out the core values that form the foundation of our profession of arms and our military culture: **engagement, righteousness and reliability.** These core values, which govern our ambition to succeed together, nourish our code of conduct and support the trust that citizens naturally place in Luxembourg's armed forces.

Engaged for our homeland, we protect human dignity and the common good with dedication and courage, and we excel, under the political authority, in the defence of our common goods.

Righteousness and integrity are at the heart of our formation, which is based on the values of equality, equity, the right measure and proportionality.

We carry out our work **reliably**, in a spirit of comradeship and respect for the dignity of the individual, with resolution, discipline and precision.

By adhering to these institutional, professional and personal values, we cultivate a serene, formative and demanding environment common to all members of the armed forces serving the Grand Duchy of Luxembourg, the United Nations, the North Atlantic Treaty Organization and the European Union.

Figure 17.1: Text of the Charter.

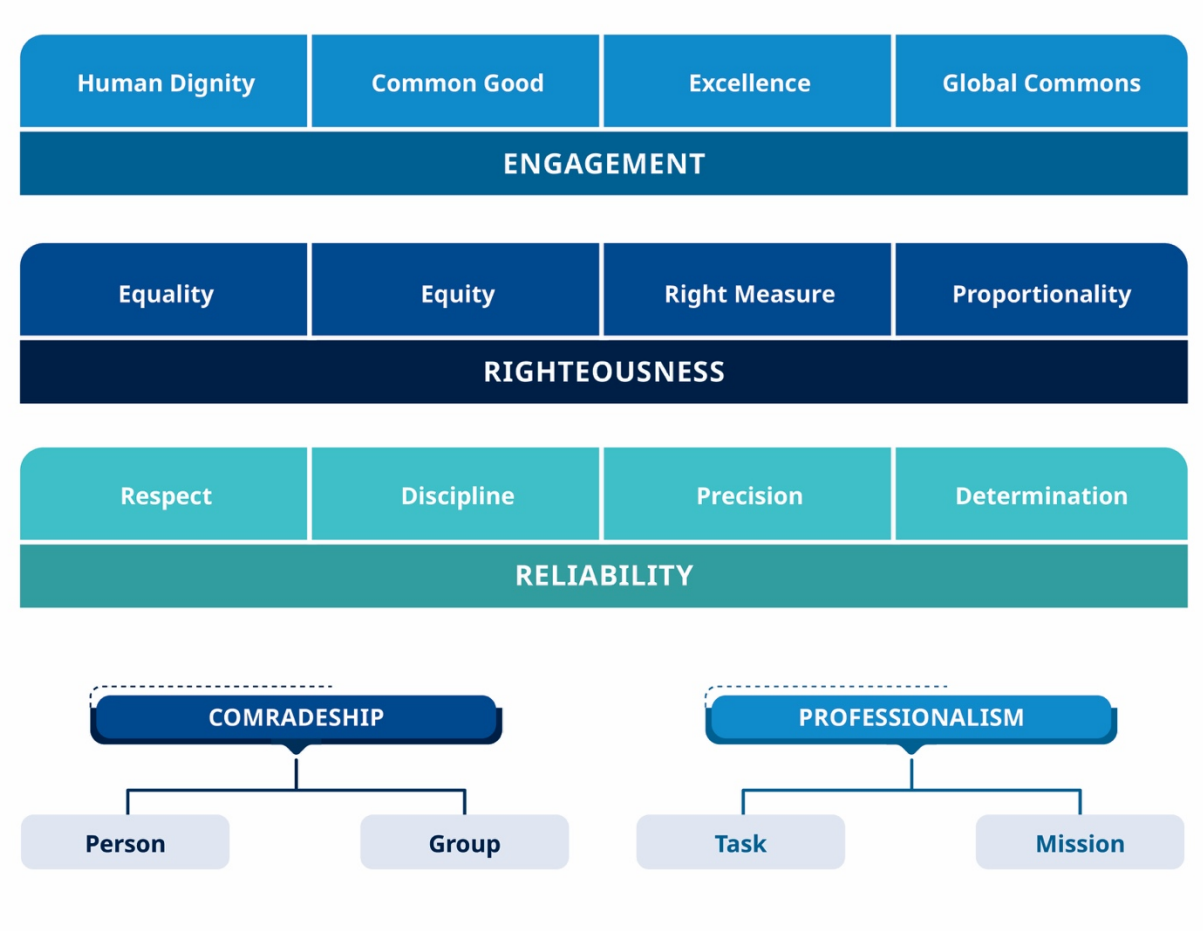


Figure 17.1: Values Table

Another result elaborated in this two-year process is the Values Table. The three horizontal lines enunciate the three super-values: engagement, righteousness, and reliability. The four dimensions distribute each of the three super-values into four dimensions: the person and the group standing for people-related values and the task and the mission standing for the work-related values.

As a pedagogical and didactical tool, the Values Table conveys a glimpse at something interconnected and interrelated. Like any table, it can be read from different angles. The super-values described in the three horizontal lines build on each other. Reliability is in each dimension the ethical starting point and required minimum, but not an end. Reliability, as an attitude and habit, is at the service of higher values which represent the ends for any soldier's engagement: the dignity of the person, the common good, excellence and the global commons. In our Western civilization, these values are commonly shared by all citizens and thus clearly express that those soldiers are also citizens in uniforms. These highly abstract and open values need to be specified in

different contexts, however. In the case of democratically controlled armed forces, the role and responsibility to specify those values rests with the political authority and the military leadership.

What part of the common good needs military protection? This can be peace at a local, regional, or national level. During a pandemic, it can be public health. The same specification goes with the global commons which must be balanced and articulated in ever new political equilibriums. Think about international waters, climate, outer space or world peace. Depending on political priorities and situational necessities or opportunities, the global commons will conflict with others. In those cases, ethical decisions need to be taken by those responsible. When and where human dignity is at threat must be openly assessed, discussed, and agreed upon. Military leaders must define the degree of excellence they want their troops to achieve under given circumstances.

The middle horizontal line in the Values Table states that all those necessary ethical assessments will be done righteously. This core ethical value offers four criteria to be considered while deciding: equality and equity when it comes to people, and the right measure and proportionality when it comes to the things to be done.

The Values Table can easily be used in formation sessions for officers and serve as a short guide when decisions become confusing. It offers a common semantic field to structure communication about complex issues.

The Code of Conduct–A Mirror

The Code of Conduct– which for the time being is available in Luxembourgish only– addresses all soldiers directly as moral subjects by offering eight *prima facie* simple self-commitments. Here, as in the Charter, it becomes obvious that ethical behaviour cannot be delegated to a faraway internal hierarchy or sometimes anonymous political level. The Code breaks the 'we' in the Charter down to the 'I' at the front line, where moral dilemmas occur and must be addressed on the spot. The eight self-commitments must not be isolated individually, because they cover the whole military ethos and represent a critical mirror for each and every soldier. Together they express what it means to be an effectual integer and loyal member of the LAF. They are not meant to blame but to motivate, first oneself and then one's comrades by serving as a good example.

It is a duty for the military leadership and those in charge of military education to 'cultivate a serene, formative and demanding environment common to all members of the armed forces.' Enabling and empowering people to behave according to outspoken and commonly elaborated values is a noble and citizen's task. Good soldiers will be good citizens in the city they serve and belong to. Didactical tools and methods can help foster a learning environment which must be governed by a continuous leadership and a commitment to provide the necessary means and put in place the structural conditions promoting and protecting the Values Charter and its Military Code of Conduct.

4. Conclusion

Our unique process Flagship Values of the Luxembourg Armed Forces was a success because it addressed the armed forces as a moral agent and encouraged its leadership to shape its ethos in a participatory and professionally designed ethical process. It could count on the active support of the members of the LAF across all ranks and the civilian employees, thus giving the Charter and the Code overall acceptance. It was only possible because the Minister of Defence invested trust and support in all those in charge of a demanding mission. Thus, a favourable environment for open dialogue and freedom of action was created and used by the military leadership to strengthen ethical awareness and moral behaviour within the LAF. The Charter and the Code reflect ethics as an ongoing and transparent process which invites soldiers and civilians to get involved as moral agents.

A process is a narrative as this contribution has shown. It integrates and excludes options and differences by creating a storyline underpinning one's identity and ambitions. Thus, we are happy to share our story of moral learning and we are eager to read or to listen to yours.

Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices, Volume II

Brussels, Geneva, 2026





Scan this **& download the full text.**

0639-26 NATO Printing & Graphics