Civil-Military Cooperation Centre of Excellence
The Hague

Building Integrity (BI)
A CCOE Fact Sheet

Introduction:

NATO recognises corruption and poor governance as security challenges. In operations this translates into actions that are designed to strengthen transparency, accountability and counter-corruption.

Corruption is understood by NATO as the "misuse of entrusted power for private benefit." It complicates every security challenge faced by NATO, it limits operational effectiveness, undermines the defence and security capabilities and reduces public trust.

"The term 'integrity' refers to the application of generally accepted values and norms in daily practice."[1] It is interconnected with the principles of transparency and accountability.

Personal integrity means for a person to believe in certain values and to stand up for them.

Organizational integrity "relates to the rules, regulations, policies and procedures defined and implemented by public institutions in various fields of operations."[2]

The NATO BI programme provides a set of practical tools and activities aimed at reducing the risk of corruption in the defence and related security sector. BI promotes the principles of integrity, transparency and accountability and provides countries with tailored support to make defence and security institutions more effective and efficient."

MISSION IMPLICATIONS

Corruption in the joint operation area (JOA) affects stabilisation missions as well as collective defence scenarios. Corruption kills and impacts operational effectiveness, represents a risks to reputation and reduces public trust. It also wastes resources and diverts resources to criminal organisation, armed opposition groups and terrorists. Corruption decreases the efficiency of local security forces and governmental institutions in establishing a safe and secure environment.

The mission must be planned and executed with an understanding of corruption as a security risk. This means identifying corruption risks and taking pro-active steps to reduce these risks. Injecting a large amount of resources into a nation with limited means to ensure transparency and accountability, especially at the initial stages of an operation, will significantly increase corruption risks. Working with local contractors also presents risks and may require specialised knowledge in preparing technical agreements and service contracts.

Effective anti-corruption efforts needs a comprehensive approach. However, the first goal of a mission should be to *do no harm*. A commitment to BI principles contributes to force security and delivers more sustainable mission results. The Commander and staff should be aware of the impact of corruption and poor governance in the JOA and the likely links to organised crime. The Commander should encourage and demand transparent and accountable financial reporting not only within the force, but also in relation with the host government and external parties.

Responsibilities in CMI

Different branches outside of J9 have a shared responsibility regarding BI. J2 has to provide in cooperation with J9 and advisors an analysis on the security sector in the JOA, including the presence of corruption. J3 and J5 have to include BI into their operations and plans. J1 and J8 have to make sure local employment and procurement do not contribute to corrupt practices. The same applies to J4 when establishing a logistics network. J7 will have to provide internal training on how recognising corruption and strategies to reduce the impact on operations; and provide internal and external training to security forces based on BI Best Practices.

LEGAL IMPLICATIONS

The UN Convention against Corruption (UNCAC) is the most important. The Commander also should be aware of the Criminal Law and the Civil Law Convention on Corruption of the Council of Europe (CoE) as well as host nation laws.

In addition to their own national regulations, laws and code of conduct, all mission personnel are responsible to act within these different laws. The Commander and the legal advisor (LEGAD) need to explain legal rules and regulations regarding outsourcing, procurement and other related topics.

Responsibilities in CMI

Different branches outside of J9 have a shared responsibility regarding BI.

J2 has to provide in cooperation with J9 and advisors an analysis on the security sector in the JOA, including the presence of corruption.

J3 and J5 have to include BI into their operations and plans.

J1 and J8 have to make sure local employment and procurement do not contribute to corrupt practices.

The same applies to J4 when establishing a logistics network.

J7 will have to provide internal training on how recognising corruption and strategies to reduce the impact on operations; and provide internal and external training to security forces based on BI Best Practices.

ASSESSMENT IMPLICATIONS

Corruption and integrity are to be included and mainstreamed into every CIMIC Assessment. "Effective anti-corruption responses cannot be designed without a thorough assessment of the problem." (Centre for Integrity in the Defence Sector (CIDS))

The presence of corrupt networks including possible financial flows need to be examined. Economic, political and social stakeholders in the JOA need to be identified. During the Comprehensive Preparation of the Operational Environment (CPOE), host government institutions, in particular the defence and related security sectors, should be analyzed for evidence of transparency and integrity policies, procedures and practices. Questions to be asked:

- ▫ *"Have senior personnel completed asset declarations?"*
- ▫ *"Is there a system in place to keep track of equipment, monitor education and training of personnel?"*
- ▫ *"Are pay scales published?"*

Preparatory assessments need to be verified and amended during the mission.

Leading International and Anti-Corruption Organizations:

United Nations Office on Drugs and Crime (UNODC): Responsible for the implementation and supervision of the UNCAC

United Nations Development Programme (UNDP): Corruption and development
CoE: Setting European norms and standards

Group of States against Corruption (GRECO): Monitoring the implementation of CoE's anti-corruption standards

OECD: Corruption and conflict of interest/public procurement

OSCE: Promoting democratic institutions and in particular democratic control of armed and security forces

World Bank: Open government, corruption and finances

Transparency International (TI): Leading civil-society organisation

Terrorism, Transnational Crime and Corruption Centre (TraCCC): leading research institute at George Mason University

NATO HQ: Responsible for the NATO BI Policy and BI activities; is the NATO Requirement Authority for BI Education and Training; provides tailored support on BI to countries, including those in which a NATO mission is deployed

CIDS: Centre for Integrity in the Defence Sector, serves as the Department Head for NATO BI Education & Training.

Points of Contact during Mission:

NATO:	BI Programme
	E-Mail: building-integrity@hq.nato.int
	Website: https://buildingintegrity.hq.nato.int
CIDS:	E-Mail: cids@ifs.mil.no
	Website: http://cids.no/
UNODC:	Corruption and Economic Crime Branch
	E-Mail: uncac.cop@unodc.org
	Website: https://www.unodc.org/unodc/en/corruption/
TI:	Transparency International Defence & Security
	E-Mail: info@ti-defence.org
	Website: www.ti-defence.org
TraCCC:	Terrorism, Transnational Crime and Corruption Center
	E-Mail: traccc@gmu.edu
	Website: http://traccc.gmu.edu

WWW.CIMIC-COE.ORG

BI is a cross-cutting topic and relates to:

1. Rule of Law: Interdependency - Necessity to work on both together to be successful.

2. Good Governance: Strong interconnection with BI; simultaneous promotion of the three principles: integrity, transparency & accountability.

3. Gender: Corruption affects all society; it is not just about money, it includes sexual exploitation; both women and men need to be part of anti-corruption measures and decisions

4. Cultural Awareness: Need to consider national and/or organisational culture to achieve a sustainable change; no one size fits all solution.

Sources of Additional Information:

UN, e.g. "The Global Programme against Corruption – UN Anti-Corruption Toolkit"

CIDS, e.g. "Criteria for good governance in the defence sector", "Integrity Action Plan: A handbook for practitioners in defence establishments"

OSCE, "Code of Conduct on Politico-Military Aspects of Security"

OECD, e.g. "OECD Recommendation of the Council on Public Integrity: Public Integrity"

The "Do's" and "Don'ts":

Do's

- Make a solid assessment of the local situation
- Respect codes of conduct.
- Observe the market and local customs carefully.
- Support national ownership of defence and security projects, but ensure international oversight and monitoring.
- Increase incentives, by recruiting locally, based on merit and integrity.
- Vet, select and train local citizens involved in the mission carefully (e.g. inform about existing rules and regulations, conflict of interest).
- Ensure oversight and reporting mechanisms are transparent and fully respected.
- Work with other stakeholders to identify local prices for goods and services.

Don'ts

- Try not to do harm and worsen the situation.
- Try not to flood the local markets with foreign currency.
- Do not disrupt the market and drive up prices for local staff.
- Do not inflate prices for locally engaged staff.
- Try not to employ private contractors as guards or entries in areas affected by insurgency.
- Try to avoid the creation of monopolies when contracting locally.
- Do not set unrealistic goals with regards to preventing and countering corruption; this is not a short term process, this work will exceed your time in theatre.
- Do not forget, resources that are diverted through corruption will likely end up supporting the armed opposition in your JOA and beyond.

WWW.CIMIC-COE.ORG

References:

- SHAPE (2012), ACO MANUAL 86-1-1
- NATO (2018), AJP-3.19 (FD)
- NATO (2010), Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices
- NATO (2016), NATO Building Integrity Policy
- OSCE (2016), Handbook on Combating Corruption

CIMIC Tasks:

☐ **Provide transparency** towards the society and function as a first point of contact/ombudsman for corruption and BI related issues.

☐ **Build a network** with IOs and NGOs working in the JOA.

☐ **Include anti-corruption and pro-integrity messages** when interacting with non-military actors.

☐ **Establish and maintain contacts** with military counterparts such as engineers and military police.

☐ **Enable communication** between logistics staff functions and potential contractors and partners in theatre (supportive contribution to host nation support).

☐ **Systematically assess and report** on practices of corruption in the JOA (e.g. through knowledge exchange with IOs and NGOs) as well as its impact on the mission goals.

☐ **Validate and update assessments** made in the CPOE in relation to corruption and integrity.

---

[1] OSCE (2016), Handbook on Combating Corruption
[2] OSCE (2016), Handbook on Combating Corruption