Analysis

Makes the Difference

Designed by Sven Dube

ANALYSIS
Makes the Difference

Foreword

Looking back on 17 years of experience in NATO civil-military cooperation I have to conclude, that over the time one main issue within this field of expertise never really changed.

We hardly succeeded to create a mission environment and sufficient trust between individuals and organizations to reach a level of information-sharing that satisfies operational requirements. There exist several reasons why critical information is not shared amongst different stakeholders although all parties are aware that it would be important to do so.

I faced this situation many times in missions and daily work. It is my firm belief that we do not face technical challenges but we have to change our mind-set from a “Need to Know” one, to a “Dare to Share” one. In order to solve current world’s crisis and even more the ones that we will face in the future, be it Hybrid Warfare, Stabilisation Operations or, at the sharp end, Collective Defence, we need to approach them with this new mind-set. In my position as the Director of the NATO CIMIC Centre of Excellence I encouraged my team to spread this mind-set by means of our trainings, publications and conferences.

Colonel Wolfgang Paulik, Director CCOE

Our Vision states: “The CCOE is a preferred network campus to connect people, share collective knowledge and gain unity of purpose in the field of Civil-Military Interaction”. “Dare to Share” is a crucial part of this vision and we, the CCOE, intend to pave the way for this mind-set.

The “Analysis Makes the Difference Workshop” was one way to do so and to foster shifting this attitude. As we perceive our Lessons Identified in the past as drivers for changes in the future, our Lessons Learned and Analysis Branch was the right choice to approach this topic.
The workshop discussed, how a comprehensive analysis can improve decision making across all levels, and how crucial information sharing is throughout the entire process. Attendees became aware how important it is to capture observations and to share them with others in order to enhance structures and processes in the future.

During those three days I took part in many controversial discussions. That also originated from the very diverse audience that we invited to this workshop on purpose. We did this, as this exchange of diverse thoughts was crucial to understand a topic comprehensively and not stay trapped within our own Bubble.

I was fully aware that a three-day workshop would not change any institutional mind-set and many good arguments have been already forgotten when I concluded my closing remarks. However, in order to keep the discussion ongoing, this report has been compiled to ensure that at least the best arguments and ideas are recorded and wouldn’t get lost.

The continuation of this important discussion more in depth is our goal. The CCOE supports the community of the interested with arguments and ideas for further discussions in their own realms, to bring the change of mind-set towards ”Dare to Share”.

Colonel Wolfgang Paulik
Director CIMIC COE

Natascha Hyrckow
Independent Advisor

All of us intervening in conflict, crisis, disaster and the aftermath of those situations feel on a daily basis the complexities faced by the impacted communities and our responsibility to understand the impact of our actions both in the immediate and longer term. Analysis and understanding of these environments, and I underline the importance of a “so what” and “recommendations” incorporated in that analysis, is our base line tool in ensuring positive interventions. I have been very inspired that the CCOE was prepared to show leadership in identifying that the worlds ever expanding complexities mean we need to get better at analysis and to invest in bringing such a broad cross-section of the interventionist community together to do just that.

Crisis has an immediacy and operational tempo that favours the reactive. Decision making needs to be agile and well informed. Analysis cannot be an afterthought or add on, it needs to be sitting at the centre of decision making conversations, be that in planning and implementation or at the strategic, operational or tactical. I totally underline the Directors point above that we must move from “need to know” to “dare to share”, a mind-set change required for all of us uniformed or civilian.

Be it Syria, Afghanistan, Mali, or any crisis, the current situation and history doesn’t change depending on the actors involved, but the lens that we view these crisis through and the expertise that we bring vary enormously. All of our interventions impact economies, power balances, the security situation and the lives of the average citizen. Becoming aware of what the different actors bring in both action and knowledge be they military, humanitarian, stabilisation, development, political, or peacebuilding improves us all. We do not need to be so naive to believe that all actions will have the same purpose to understand the benefits of improved understanding.

Politics, communities and life are about people and relationships. This workshop began a process of bringing together professionals from many backgrounds to improve our individual and overall performance. That it is happening at a time where the UN is reforming its peace and security architecture with a focus on better analysis and better integration across the intervention spectrum reinforces the impact of the CCOEs leadership.

Many thanks for the opportunity to be involved.

Natascha Hryckow

Content

Introduction

The Workshop “Analysis Makes the Difference” from 16 - 18 October 2018, was organized together with partners by the Civil-Military Cooperation Centre of Excellence.

At the workshop 118 experts from the military and civilian sectors participated. The participants came from 31 countries and 65 military and civilian organizations.

The overall aim of the workshop was to strengthen cooperation between military and civilian spheres by enhancing mutual trust and confidence between NATO, its partners, and other international and local actors.

The workshop overall topics were:

1. Military and Civilian approaches to Analysis of the Civil Environment - including Conflict Analysis;
2. Discussions on Collective Defense, Resilience Building, Stability Operations with illustrative cases from Mali, Syria and North Eastern Europe Areas;
3. Enhancing the CIMIC Lessons Learned Community/Mindset; and
4. Improvement of concepts, and architectures for Civil-Military Information Sharing.

The Workshop had a broad focus on the purpose of identifying areas that in all four topics could be investigated more by organizing further deep-dive workshops, conferences etc.

The workshop was divided into three syndicates as follows:

Syndicate 1: Comprehensive Analysis.

Aimed to facilitate the sharing of knowledge and information among diverse actors and raise awareness of different analysis approaches.

Syndicate 2: CIV-MIL Lessons Learned.

Aimed to conduct bespoke training for CIMIC Lessons Learned actors and initiated a CIMIC Lessons Learned Community, with particular attention given to structures, tools, processes, and training.

Syndicate 3: CIV-MIL Information Sharing.

Aimed to improve the capabilities of military organizations to share and manage information on the civil environment with humanitarian actors in an effective, efficient and appropriate manner.

Participants included CIMIC and Civil Affairs officers, military personnel from different forces and of varying rank, academics and humanitarians. It should be noted that these sectors are not homogenous; within each, there are many sub-groups that have different mandates, approaches and internal challenges surrounding information sharing (for example, J2 and J9).

An important key objective of the event was for the military and the non-military organizations to meet, exchange knowledge and build relationships so that over time all stakeholders have a common understanding of each other and that a strengthened cooperation is necessary for the future. The workshop has shown that the CCOE is an appropriate independent networking hub to discuss topics of mutual interest for the military and civil sphere.

Introduction of Speaker

Lieutenant General (retired) Ton van Loon

Lieutenant General (retired) Ton van Loon is a commander from The Netherlands who acts as Senior Mentor on NATO exercises.
Mr. van Loon enrolled in the Koninklijke Militaire Academie in Breda in 1977. Starting in 1990, he attended the Royal Netherlands Army Staff College at The Hague, following staff officer training courses. In 1995 he attended the British Army Command and Staff College, after which he returned to international military cooperation with a staff position at the I. German/Dutch Corps in Münster. As Battalion Commander he was deployed to Kosovo in 1999 as part of the KFOR1 Multinational Brigade South (under German command).

On November 1, 2006 until May 1, 2007 Mr. van Loon took control of the International Security Assistance Force (ISAF), Regional Command South (RC-S). From April 13, 2010 until September 25, 2013, he commanded I. German/Dutch Corps. On April 1, 2010 Mr. van Loon was promoted to Lieutenant General ahead of his April 13 assignment to the I. German/Dutch Corps as Corps Commander. Upon his retirement he was awarded by Germany with the Grand Merit Cross with Star Order of Merit of the Federal Republic of Germany and he was promoted to Officer in the Order of Orange-Nassau with swords.

Mohan Ramesh Rajasingham

Mr. Mohan Ramesh Rajasingham was appointed Director of OCHA's Coordination Division in September 2018.

Mr. Rajasingham's career in the field of humanitarian affairs and with the United Nations system spans over 25 years, and includes assignments in Headquarters as well as in crisis settings, with OCHA and UNICEF.

Most recently, he served as Deputy Humanitarian Coordinator for the Syria Crisis. Prior to that, he held such senior appointments as the Director of the Secretariat of the Secretary-General's High-level Panel on the Global Response to Health Crises and the Head of Office of the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) in the occupied Palestinian territory. He also headed OCHA's largest field operation, in Sudan, where he was also responsible for coordination of relief operations and negotiating humanitarian access in Darfur, as well as the transition situation in what is now South Sudan.

His field assignments also include Afghanistan and Bosnia Herzegovina. At Headquarters, he has served in various capacities in the response, protection and policy activities of the Organisation.

Originally from Sri Lanka, Mr. Rajasingham is an economist trained in the United Kingdom and the United States of America. He is married with two children.

Iulian Chifu

Iulian Chifu is an Associate Professor at the National School of Political and Administrative Studies in Bucharest.

He is the founder of the Center for Conflict Prevention and Early Warning Bucharest. Between 2011 and 2014, Mr. Chifu was the Counsellor for Strategic Affairs and International Security to the Romanian President.

He acted as an Advisor for foreign policy, security, and defense to the Vice-President of the Romanian Senate (2006-2011). Mr. Chifu specializes in conflict analysis, crisis decision making, and the post-Soviet space.

Among his books, we can mention: The Changing Face of Warfare in the 21st Century (Iulian Chifu, Gregory Simons, 2017), Prospective on Ukraine crisis: a trilateral approach (Iulian Chifu, Oazu Nantoi, Alyona Getmanchuk, 2015), The East-West Black Sea – Caspian Sea Strategic Corridor (Iulian Chifu, Narciz Bălășoiu, Radu Arghir, 2014).

Natascha Hryckow

Natascha Hryckow is an experienced leader of multilateral interventions with a particular interest in conflict and post conflict environments.

Experiences across the European Union, (including Political Director and Head of country for Somalia and Kenya for EUCAP Nestor), the North Atlantic Treaty Organization (NATO), (including as the Political Director for the SCR in Afghanistan), the UN, and government have shaped her perceptions of current day interventions.

Most recently she has been working with WHO as their first conflict specialist and has been responsible for developing and introducing the concept of “delivering in conflict” as a speciality. This role has had a particular focus on Syria, Iraq, Libya, Yemen and Somalia and has included operational tasks such as coordinating the Raqqa trauma response.

Michael A. Charlebois

Michael A. Charlebois served nearly 28 years in the United States Army with a wide range of specialties from initial entry as an enlisted Combat Engineer and later Military Police to commissioning in the Medical Service Corps where he served as a platoon leader in the 1/508th Parachute Infantry Regiment, before branch transferring to Aviation where he commanded in the 101st Air Assault Division and served in the 160th Special Operations Aviation Regiment. His final Area of Concentration as a Civil Affairs Officer (CAO) found him commanding in combat along the Iraq-Iran border. Prior to retirement, Michael served as the Director for Global War on Terror for US Southern Command, and led Doctrine, Training, Personnel, and Force Modernization for the Civil Affairs Proponent.

Michael terminated his military career abruptly in order to pursue his current position as Deputy Commandant for Civil Affairs.

His current duties and responsibilities as the Deputy Commandant for Civil Affairs at the United States Army John F. Kennedy Special Warfare Center and School include all DOTMLPF-P[1] considerations and force modernization for a total Civil Affairs force consisting of more than 7,000 officers and soldiers.

Michael's military education includes Naval Postgraduate School Special Operations/Low Intensity Conflicts, Command and General Staff College at the Western Hemisphere Institute for Security Cooperation (formerly School of Americas), Joint Professional Military Education Level II, High Risk Level C SERE, Joint Air Combat Controller Course, Joint Air Operations Staff Course, and Joint Firepower Controller Course.

Michael's military awards and decorations include the Legion of Merit, two Bronze Stars, the Joint Meritorious Service Medal, three Army Meritorious Service Medals, Joint Commendation Award, and Army Commendation award. Additionally he holds the Expert Field Medical Badge, Aviation Badge, Airborne, Pathfinder, and Air Assault badges.

[1] doctrine, organization, training, materiel, leadership and education, personnel, and facilities

ANALYSIS
Makes the Difference

Our Partners

Setting up this workshop and writing this final report required an exceptional commitment. None of this would have been possible without our partners.

We want to express our gratitude to Natascha Hryckow, Masayo Kondo Rossier (UN OCHA) and Rachel Agelou who supported us in developing a concept for this workshop and finally conducting it. Always kept us on track with their critical feedback and provided a different point of view.

Thank you to Angeliki Nika and Margaux Boffi from ACAPS, giving an interesting insight into ACAPS's analysis methodology and leading a sub-syndicate in a diverse Civil-military environment.

Special thanks to Erik Agoglia (iMMAP) and Martin Fisher for bringing in their exceptional experience as analysts in different conflict areas, but especially from Syria. You added practical experience and made it a hands on experience.

Without the support from JALLC, in person LTC Sinisa Cular and LTC Francesco Pepe, the syndicate on Lessons Learned training would never have been possible. Thank you very much for your outstanding performance.

LTC Lars Nielsen from Multinational Corpse Northeast was assigned last minute to this task and performed exceptionally well. His introduction and explanations to Resilience triggered many fruitful discussions during the workshop and for the future.

We don’t want to miss the chance to thank Charles “Bill” Robinson and Tom Jarrell (US Joint Staff), not only for their performance during the workshop but also for their effort and cooperation during the FMCM project. The outcomes of this project are important baseline documents in the future, especially when it comes to civil military information sharing.

The first impression report and the final report would never exist without the tremendous job Pieter Griffioen, Kendra Schreiner and Laura Dominguez Pires did in capturing all the outcomes of discussions and working group sessions in Syndicate 1. Thank you very much for your effort.

Finally a very special thanks to Samantha Hewitt, who had the challenging task to include all comments from our partners into the draft versions of the report and made it a ready to publish product. You did a fabulous job.

Syndicate 1 - Comprehensive Analysis

Syndicate 1, Comprehensive Analysis, focused on how to achieve a comprehensive approach to analysis, which takes into account the knowledge, expertise, and methodologies of civil and military actors through the sharing of analysis and information. The syndicate aimed to raise awareness on analysis approaches and the impact on decision-making across the strategic, operational and tactical/programmatic spheres.

The expected outcome was to:

1. Provide a report identifying solutions for the development of a platform to link analysis and decision-makers from different stakeholders;

2. Foster a common understanding of comprehensive analysis; and

3. Identify areas of cooperation that will allow the development of a standardized conflict analysis/information system across all sectors in the future.

"The goal was to leave with concrete advice on how to proceed, rather than have another stand-alone event without sustainability".

Colonel Wolfgang Paulik,
Director CCOE

In the context of hybrid warfare and intrastate, protracted conflict, crises have become more complex; civilians and civilian organizations are playing an increasing role within conflict settings, and militaries are focusing on the protection of civilians and societal resilience to help fulfill their mission. An actor's perspective influences the analysis. One may focus on the scope and extent of humanitarian needs within a crisis, whilst another may focus on the crisis itself. As a collective community, mutual benefit could be gained by sharing these analytical perspectives. In this context, there is an urgency to have the best possible analysis; the problem must be correctly identified in order to develop the correct solutions. However, identification is not enough; analysis must be a dynamic process whereby decision-makers are involved throughout, providing clear direction to analysts to ensure the product of analysis is of good quality, relevant and timely.

Globally, conflict trends have led to a growing demand for comprehensive analysis approaches from both civilian and military actors. From a military perspective, the expansion of hybrid warfare has brought the need for comprehensive analysis to the fore. The start of a conflict is less defined, as information and messaging can be used to influence public perception and push the limits without crossing a line into an Article 5 situation. As such, resilience has become increasingly important. In order to reassure the public and counter disinformation, military actors must understand the civilian environment, which requires the sharing of information with non-military actors. From a civilian perspective, intervening and delivering projects in a conflict setting remains a work in progress.

Most humanitarian and development doctrine began in natural disasters. Cooperating with other sectors in analysis can, therefore, help to fill gaps where expertise is lacking as well as provide perspective and triangulation of existing analysis, increasing reliability. In addition, civilians require logistical information in a conflict setting for pragmatic purposes, such as the status of transportation routes. Regardless of respective mandates, all conflict actors must realize they need to talk to others because they might not be right. It is essential to ask the right questions, and not be reluctant to admit there might be new and different information out there.

The issue is not a dearth of tools and methodologies; rather, it is a lack of joined-up analysis and sharing of perspectives and information. To explore how this can be amended, Syndicate 1 heard from civil and military experts and decision-makers regarding their experience, where they see challenges, and how the issue is currently being tackled.

This dialogue demonstrated the value of cross-sector collaboration as participants were exposed not only to new methodologies but viewpoints and perceptions of the issues at hand.

> *“The most important element for decision-making is that we realize we might not have the answer.*
>
> *Getting the answer is relatively easy if you ask the right question, but we are very reluctant in asking the questions.”*
>
> Lieutenant General (retired) Ton van Loon

Lieutenant General (retired) Ton van Loon

Key Concepts

While military and civilian actors need not share the same goals, clarity of definition and purpose are essential components of constructive dialogue and cross-sector cooperation.
Based on discussions at the workshop, this report uses the following loose definitions:

Comprehensive Approach - A response to crisis situations that combines political, civilian and military instruments, with all actors contributing in a concerted effort to achieve and maintain peace, security, and stability.

Analysis - The breaking down of something complex into simpler and more basic elements to learn about its parts, what they do and how they relate to each other. Information itself is not analysis; it is the breaking down of information and relating it to other data.

Comprehensive Analysis - The bringing together of political, civilian and military analyses to ensure that information is not missed and different experiences and perspectives are taken into account. This approach recognizes that the operational environment is a complex, interconnected system and effective decision-making requires holistic understanding. This can be achieved through different levels of cooperation tailored to the situation, including sharing raw data, sharing analysis or conducting analysis jointly.

Assessment - In contrast to analysis, assessment involves making a judgment about something and deciding its importance. When an assessment is made without accurate analysis, the result can be poorly informed and ineffective decision-making.

Resilience (NATO) - The ability of host nations to resist and recover easily and quickly from shocks and stresses, combining civilian, commercial and military factors, and resources.

Resilience (Humanitarian) - The ability of households and communities to meet their basic needs in a sustainable way and without reliance on external assistance so they can resist, absorb, accommodate and recover from stresses quickly.

The Current Situation & Key Challenges

Information and analysis sharing mechanisms do exist in current crises. However, it is often at the tactical to the operational level, with little sustainability or depth. In Mali, for example, personnel from the military will participate in briefings of the Special Representative of the Secretary-General and humanitarians will attend military briefings. This type of arrangement is not an institutionalized, standard approach and is often dependent on the situation and leadership. When the situation changes, perhaps due to champions of the approach leaving the mission, collaboration is often disrupted or ceases. It is clear that institutionalization of comprehensive analysis is needed to make this practice routine and sustainable. Furthermore, if analysis is to truly be comprehensive it must go beyond daily logistics challenges and consider not only the political, civil and military silos; but also the tactical, operational and strategic levels.

> *“The military also has a role to play and we have seen it in natural disasters and now in peacekeeping missions.”*
>
> Mohan Ramesh Rajasingham
> Director UN OCHA Coordination Division

Throughout the workshop, many challenges - some on the civilian side, some military and some common to both, were identified:

Over-classification - An over-developed culture of secrecy within military bodies was identified as a key obstacle to sharing information. Previously public information used in analysis will often become classified, rendering it useless for exchange.

Organisational culture - There are many in the military that maintain a mission-centric focus that lacks adequate consideration of the civilian sector. The civil sector, with a view to maintain impartiality, avoid activities which could be seen as ‘political’ and focus on reactive, immediate needs-based interventions, which can lack consideration of longer-term strategic implications. These cultural tendencies from both actors can impede a comprehensive approach.

Lack of trust - Civilians continue to view military personnel with suspicion, questioning their motives and ultimate aims. Humanitarians also avoid association due to fear of how it will affect the way they are perceived by the local population. Military personnel feel that any information shared with humanitarians will be broadcast widely and used opaquely.

Lack of value placed on long-term analysis - Both military and civilian actors are more practiced at operational level analysis and collaboration, but a limited focus on larger visions and trends deters comprehensive analysis at the strategic and tactical levels.

Different mandates - Two extremes of the perceived purpose of comprehensive analysis identified are: to gain and use knowledge about the civilian environment to support the mandated mission; and to find synergies between civilian and military goals in order to collaborate to minimize and mitigate the effects of conflict. These different views lead to the collection and emphasis of different types of information, hindering effective sharing and development of a holistic picture of the situation.

Resources and Training - Stemming from a lack of organizational value placed on analysis above the operational level, it is under-resourced, with entire country operations employing one or two analysts and a lack of training provided. It was stated during the workshop that military resourcing for analysis exceeds that of the civilian world.

Short deployments - Military deployments of only three to six months were identified as hindering in-depth and comprehensive analysis as the required relationship-building with both civilian organizations and locals is next to impossible.

> *“Information by itself is not valuable if you don’t understand it in a cultural context.”*
>
> Michael A. Charlebois

Michael A. Charlebois, Deputy Commandant for Civil Affairs at the United States Army John F. Kennedy Special Warfare Center and School

Analysis Approaches

Stakeholders working in or analysing crises in different geographical areas (Mali, Syria, Eastern Europe, and others) gathered to identify synergies and challenges in collaboratively working towards a comprehensive analysis of a crisis.

Key questions considered by syndicate participants included:

1. How can we get a better and more comprehensive picture of conflict environments?
2. What are the main challenges in analysis and cooperation in it?
3. How can analysis be most effectively translated into decision-making?

The workshop was broad, covering 'analysis' as a whole. While this was a valuable exercise to gain an understanding of the many different viewpoints and challenges that exist, participants at times struggled to reach a mutual understanding as they focused on different levels of analysis and stages of conflict.

As such, comprehensive analysis discussions should begin by clarifying the level of decision-making and the stage of the crisis. Relatedly, the customer of the analysis must be clearly defined in order to produce a product that meets the customer's needs, otherwise, it risks being sidelined and having minimal influence on decision-making.
The three main levels of decision-making for analysis are strategic, operational and tactical or programmatic; at each, the type of information collected, analysis methodology and end product will differ.

At a **strategic level**, which is concerned with prevention and long-term goals, a deep understanding of all involved stakeholders and a clear vision are essential. Preparedness and forward-looking analysis are key at this level. Currently, most analysis is reactive, and understanding a larger vision and the trends is a work in progress.

At an **operational level**, where decisions relate to the implementation of strategic decisions, technical skills such as data management, analysis tools and knowledge of methodologies are important.

The humanitarian analyst community has improved greatly in these areas but still lacks the capacity to meet the immensity of the challenge.

At a **tactical or programmatic level**, in which day-to-day and short-term decisions are made, building relationships with the right people is key in order to negotiate access to certain areas and maintain an adequate security presence to operate in high-risk areas.

Additionally, different stages of crisis will have different ramifications for analysis and the willingness of actors to share information. For example, at the deployment stage information needed will revolve around access, legal ramifications and so forth, rather than community-level data. In a protracted crisis, such as Syria, where it is at the stage of ending set-piece of military operations, required information includes: the status of regional partners; what the re-established state will mean for communities; power dynamics and resources at the community level; and how humanitarian interventions could affect these and broader dynamics.

While the levels of analysis are interconnected, clarifying at what level the focus lies helps direct the analyst community and enables better sorting of a large amount of collected information. Often, the challenge for analysts is tailoring information from different levels to the decision-makers' needs during the different conflict stages. To make these different stages and types of analysis more tangible and to explore the challenges and different ways of approaching analysis in different crises, Syndicate 1 divided into three sub-syndicates that each examined one analysis methodology and scenario in-depth. The outcomes of these sub-syndicates are discussed below.

Analysis Method for Humanitarian and Stabilization Operations

The first sub-syndicate introduced the fundamentals of the analysis process as can be applied across audiences that span programmatic Non-Government Organizations, stabilization actors, diplomats, UN directors, and the donor community. Specific tools used by different organizations should not be confused with the fundamentals of the analysis process.

A representative from iMMAP provided examples of their Syria work highlighting that methodologies and approaches must be flexible enough to support and guide decision-making across the strategic, operational, and programmatic levels. iMMAP is an international NGO that provides information management services for humanitarian partners, with a special focus on programming whilst also catering to the needs of development and governmental organizations. The purpose of the analysis is to support and guide strategic and programmatic decision-making.

iMMAP's process consists of five main steps:

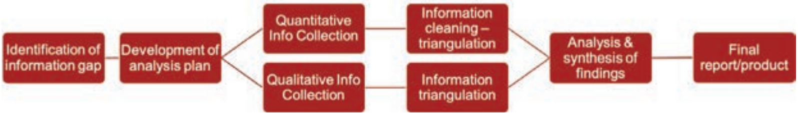
1. **Identify the information gap** that the analysis aims to fill.

2. **Develop an analysis plan** to obtain the information required by the analyst. This plan is critical to concretely define what elements are desired in the analysis and work backward from there.

3. **Collect the information** on a qualitative or quantitative basis. Clean and confirm the information through triangulation.

4. **Synthesize the findings and analyse the obtained information** in order to extract valuable knowledge for the decision-maker.

5. **Tailor the analysis to the needs** of the audience and decision-maker, which can be done in the form of a report, graph or map.


Identification of information gap
Development of analysis plan
Quantitative Info Collection
Qualitative Info Collection
Information cleaning – triangulation
Information triangulation
Analysis & synthesis of findings
Final report/product

Participants were asked to apply this process to the case-study of Syria, specifically on broad strategic questions around borders and governance structures. The aim of this exercise was to anticipate or predict the situation in these two issue areas for 2019 by identifying current information gaps and brainstorming ways to retrieve this information. This process provides value as it does not pre-determine targets or indicators and can thus be used by varying sectors. The methodology is also focused on strategic-level decision-makers, as the final product is tailored to their needs and provides forward-looking analysis that enables them to influence future issues.

During the brainstorming exercise on analysing borders, multiple information gaps were identified by the different sub-groups. This included, among others: which closed border crossings will reopen and when; whether trade between Syria and its neighbours will resume; how the needs of population centers will be met; whether Turkey will close the border during the last offensive; and whether refugees will be forced to return.

The governance structures mentioned during the group exercise in Syria were under ISIS (formerly), rebel, Syrian Government, Syrian Democratic Forces (SDF), or Turkish control. The main information gaps identified included whether conscription requirements will change, whether the professional class will return once fighting stops, whether the US support for the SDF will continue, and what the resumption of services will look like. In general, the two exercises revealed multiple information gaps which, in practice, would lead to the formation of analysis goals, followed by the analysis steps described above.

Key findings from the sub-syndicate were:

1. The need to look at the situation/region in a holistic and comprehensive manner.

2. The need to identify the goals of the external players in Syria.

3. The need to look at what a likely end-state of the Syrian conflict would look like.

4. The importance of thinking about how the transition to the end-state will look like.

5. The importance of identifying and engaging all key stakeholders in the conflict (including Russia, China, and Iran).

This exercise primarily focused on the first and second steps of the analysis process in order to emphasize the importance of pre-planning in order to ensure analysts, programmers, and decision-makers are asking the right questions needed to make the right decisions. This led to questions which could not be answered in the workshop itself but raised important questions around our current procedures, methodologies, and structures with regard to conflict analysis in Syria.

The problem of a conflict needs to be identified appropriately and accurately, without analysing topics based upon preconceived biases and assumptions. Are we asking the right questions and are we prepared for the honest answer? It is necessary to utilize analysts to develop and drive the identification of problem sets that require analysis based upon their tactical and operational experience and insight.

> *“In a way, it’s not so much what’s the most important analysis; it’s what’s the most important question that we need to answer.”*
>
> Natascha Hryckow
> Independent Advisor

This process is time-consuming and occurs in dynamic and evolving situations requiring continual review, especially for strategic questions. To maintain a resource that is able to answer those kinds of questions require adequately funded structures that are appropriately networked with clear lines of communication, staffed by a diverse range of qualified and competent expertise. The current environment lacks a mechanism for objectively analysing the context across the strategic to programmatic spectrum.

This mechanism would work best as a consortium or network of organizations and analysts that receive sustained funding to conduct in-depth and long-term research and analysis in support of decision makers and programmers.

In order to analyse the context of the Syrian conflict objectively, it is necessary to overcome the perceived biases of a civil and military actor divide. Furthermore it is not sufficient to engage only with actors that respective organizations are accustomed to cooperating with; for example, Operation Inherent Resolve (OIR) coalition, western and allied militaries, International Organizations, Non-Government Organizations, and Government Organizations. Comprehensive analysis requires quality networks and communiqué for the purpose of meaningful coordination with all stakeholders in this conflict, including representation from Russia, Iran, China, and Hezbollah in order to continue operational activities.

NATO Analysis Method – Seven Baseline Requirements for Resilience

For NATO, resilience is the ability to resist and recover quickly and efficiently from shocks and stresses, combining civilian, economic, commercial and military factors and resources. This is achieved by enhancing civil preparedness within public and private sectors, supported by military capability and capacity.

Resilience occurs at four levels of society: being the individual level, societal or community level, state level, and the regional or global level. The range of security threats requiring prevention and response through resilience measures fall into two categories of natural and man-made disasters. Climate change has seen an increase in natural disasters and the requirement to prepare society at all levels in an effort to minimise disruption and have measures in place to return as quickly as possible to normal life post a disaster event. Man-made disasters encompass disaster resulting from conflict and terrorism, hybrid warfare and emerging cyber and cyber-space threats. Such complex challenges to collective defense drive a necessity for a collaborative resilience approach to counter and withstand attacks.

NATO first incorporated resilience into its activities during the Cold War to support resistance to crisis situations. In recent years, the NATO Readiness Action Plan was introduced at the 2014 Wales Summit and the 'Commitment to Enhance Resilience' initiative was adopted by the Alliance during the Warsaw Summit of 2016. The NATO's Civil Emergency Planning committee is key to resilience building, contributing to NATO's strategic objectives with civilian expertise and capabilities. The European Union finances numerous programs to build resilience and has increased cooperation with NATO in response to rapidly increasing contemporary challenges including hybrid and cyber threats.

“It is important for NATO to share information and share knowledge, because when our soldiers are on mission, we can work together with the civilian actors to achieve common goals.”

Dirk Brengelmann
Ambassador
of Germany in The Netherlands

The United Nations similarly are active in promoting resilience with a focus on natural disasters, livelihoods, climate-change, protracted crisis, conflict prevention, and peace-building.

As with analysis, a comprehensive approach to resilience is needed. NATO is working closer with political and military organisations as well as allied countries and the private sector to better bolster resilience. Specifically, in the CIMIC context, NATO has developed the RAP in support of civil-military resilience, requiring Allies to have current crisis-response, civil emergency, and civil defense measures.

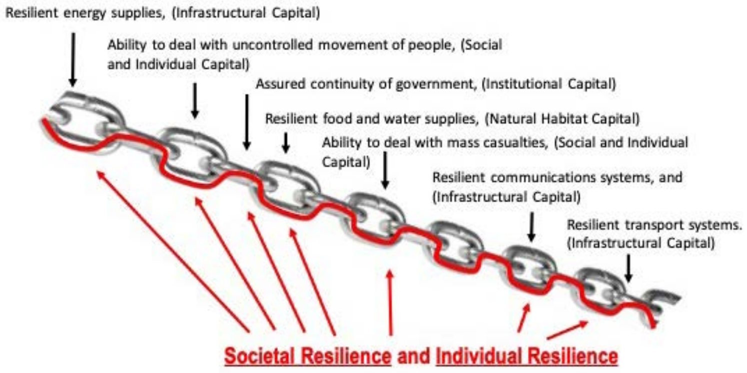
Further background information on resilience can be found in the ‘Resilience – fact sheet, on the CCOE webpage. (or Appendix of this book)

In order to measure resilience at the various levels of society, NATO collects information on seven baseline requirements:

1. Assured continuity of government and critical government services
2. Resilient energy supplies
3. Ability to deal with the uncontrolled movement of people
4. Resilient food and water supplies
5. Ability to deal with mass casualties
6. Resilient communication systems
7. Resilient transport systems

The presentation provided on resilience referred to an unofficial eighth factor looking at the resilience of the individual in the society. This looks at the resilience of the individual in the society, namely their ability to resist manipulation through misinformation in media and social media. For NATO, this is not an official baseline requirement, however, considered one of four levels of society at which resilience can be observed – societal, state and regional resilience being the others. NATO sees the need for developing a message to counter misinformation and reassure the population. Civilians and government should create this message, however, NATO can cooperate to deliver it.

The seven baseline requirements


Resilient energy supplies, (Infrastructural Capital)
Ability to deal with uncontrolled movement of people, (Social and Individual Capital)
Assured continuity of government, (Institutional Capital)
Resilient food and water supplies, (Natural Habitat Capital)
Ability to deal with mass casualties, (Social and Individual Capital)
Resilient communications systems, and (Infrastructural Capital)
Resilient transport systems. (Infrastructural Capital)
Societal Resilience and Individual Resilience

Sub-syndicate participants discussed what is missing from this tool and took part in a simulation based on the Eastern European context in which the tool was applied. The aim of this activity was not to cover the vast and complex topic of resilience, rather identify how early and comprehensive analysis of resilience indicators can benefit actors and decision-makers in taking preventative action. In measuring resilience through analysis, the syndicate discussed factors that could prevent conflict or mitigate its effects, also considering broader analysis is possible through layering with other tools, such as PMESII (Political, Military, Economic, Social, Infrastructure, Information). It was also agreed the tool is missing some important aspects. It is quite technical and human factors must be added to each technical aspect. Additionally, societal level tensions, such as the integration of ethnolinguistic minorities, culture, the popular perception of NATO, and legal institutions were highlighted as missing. Additionally, the tool focuses on the state level and relies on member states to provide data, which may affect reliability due to sensitivities around information sharing.

Specific challenges to analysis in Eastern Europe were also identified:

1. Hybrid Warfare – cyber, economic and diplomatic measure to undermine democratically chosen governments.

2. Disputes over history and identity – three Baltic States have chosen their path of independence and their last conflict was with the occupying Soviet Union. This disparity is still creating friction with Russia.

3. Energy supplies – diversification of energy supplies to safeguard from using gas as a leverage.

4. Functioning governments that have ultimate decision-making power - these decide whether to share information and whether to accept the findings of analysis, which limits translation into effective action.

Future work calls for the development of specific indicators for each resilience requirement, which will guide the assessment. The implementation of resilience requires further recognition of responders in case of events that affect the resilience of a state and also propose mechanisms for cooperative work to raise resilience.

ACAPS Analysis Method – Qualitative Methodology and Global Crisis Severity Index

The third sub-syndicate introduced the Assessment Capacities Project (ACAPS) quantitative methodology for their Global Emergency Overview, a weekly update that provides a snapshot of current humanitarian priorities and recent events, and for their new Global Crisis Severity Index. Using a retrospective approach, this index attempts to rank the severity of crises in order to provide evidence to inform the needs-based global allocation of resources, strengthen global level risk-based planning and allow organizations to combine their own data with global level security and risk data. It focuses on three main pillars: the geographical and human impact of the crisis, the humanitarian conditions, and the complexity of the emergency. These are further divided into 19 core indicators and 9 access indicators. Along with the presentation of the methodology, the sub-syndicate identified different types of biases (selection, social and process bias) and problems with the reliability of data that can limit the accuracy, and therefore the usefulness of the analysis.

Mali provided a good case study for the methodology as the crisis has many intertwining factors that affect stability. Monitoring the dozens of factors that can adversely affect the conflict situation, such as food insecurity and internal displacement, is critical to provide a comprehensive approach. Through a role-playing activity divided into different types of emergencies (floods, food insecurity, and drought), participants were tasked with drafting an analysis from the information provided from the ACAPS methodology. Mali has undergone multiple challenges since the conflict began in 2012 with the rise of religious extremism, national and international displacement of persons, food insecurity and the effects of climate change such as intensified droughts. Additionally, Mali and the Sahel represent a key region for European interests. As such, the humanitarian and military presence is constant, especially in the northern regions.

Sub-syndicate participants discussed the importance of understanding the different factors assessed in humanitarian overviews that can threaten the stability of the region; for example, internal displacement that can influence food insecurity and thus cause further social disruption. The ACAPS needs assessment overview is not only applicable to humanitarians; for example, this information could be used by military forces to prevent forecasted disruptions or the spread of radicalization to the central and southern regions of Mali.

A role-playing exercise allowed participants to practice identifying different types of biases (selection, social and process) and problems with the reliability of data that can limit the accuracy and therefore the usefulness of the analysis.
The sub-syndicate noted that the retrospective methodology limits its usefulness for forecasting conflict trends, at least until more historical data is accumulated in the years to come that enables the identification of patterns for modeling. Further, the approach is mainly aggregated at the state level and must be supplemented with other data for local level use. The ACAPS methodology also has several advantages, including its transparency and independence from political influences through independent funding sources and its holistic nature.

Positively, the methodology is transparent, attentive to bias and various actors can use the application in the field. The multi-sectoral analysis enables crisis responders to better understand and address the affected population. However, the analysis is mainly aggregated at the state level and must be supplemented with other data for local level use. The retrospective approach of gathering information and mapping it using proxy indicators does not provide forward-looking analysis to assess tendencies in the near future.

The discussion during the workshop showed, that ways of work do not differ significantly; however, scope and level of analysis differ between different stakeholders. Therefore it is important to develop a common understanding of what analysis is and how it is used. All analysts face similar challenges during their analysis, no matter which organization they are working for. One of the major challenges in this context is the difficulty of data sharing between different stakeholders and understanding different analysis languages used.

> *"When we look at differences of analysis, it is not about methodology, it is about lenses and preconceptions."*
>
> Natascha Hryckow
> Independent Advisor

Outcome and Findings

The syndicate discussions were broad, looking jointly at strategic, operational and tactical levels. There is a greater challenge in understanding the requirements or outputs across the strategic to the tactical sphere rather than between civil and military actors. Going forward, narrower and more focused workshops and meetings will identify concrete solutions to enable comprehensive analysis, and refine that which exists, but is yet to be mainstreamed.

The points for entry in collaboration are:

1. **Topics of interest -** This may be at all levels of analysis and enables stakeholders that are not natural partners to work together.

2. **Problems and challenges -** Often, humanitarian programmatic Non-Government Organizations, military actors and analysts face very similar challenges and can work together and share information to help overcome these. For example, access to a restricted area.

3. **Areas of operation -** When the area of operation overlaps for different stakeholders and their mandates, collaboration is logical and indeed necessary to obtain a holistic picture.

4. **General methodological flow -** The general flow of analysis is similar between stakeholders in many circumstances.

5. **Operational and/or programmatic end goals -** While at a strategic level different stakeholders may have diverging objectives due to different mandates, the end goals might be quite similar at an operational or programmatic level. For example, the resumption of services to a certain area.

> *"Analysis, assessments and these activities have changed a lot in the last 25 years. It has become much more rigorous, much more evidence based, much more objective."*
>
> Mohan Ramesh Rajasingham
> Director UN OCHA Coordination Division

The challenges to collaboration are:

1. **Analysis tools and methodologies -** While these may differ, it is often only due to different ways of viewing the same information since it must be catered to different decision-makers.

2. **Implementation of information collection practices** - While the ways of collecting information may differ greatly between the military and civilian organisations (as well as within these groups, such as between J2 and J9), the actual information collected is often similar in nature, reinforcing the need for information sharing.

3. **Resources and funding capabilities -** Civilians do not have the same level of access as the military to satellite imagery, classified information and other resources for information gathering, and must always fight for analysis and sell their case. Sharing of the military's more professional conflict analysis could elevate humanitarian capabilities and avoid duplication of efforts.

4. **Lenses of analysis** - How events unfolding on the ground are viewed differs depending on the stakeholder and analyst as each looks at information according to their interests and aims; however, they often analyse similar information and events in the end.

5. **Language** - One of the starkest differences between actors is language. Often, actors are speaking about the same thing but still not connecting. It is therefore important to be familiar with the language of other sectors in order to achieve mutual understanding.

More actors and stakeholders are needed at the table. Humanitarian, development, academic and political representatives are required to share analysis from their perspectives, ensuring essential viewpoints and understandings are not missed and become an accepted essential element in the decision-making process across all levels. No one methodology, whether due to a flaw, limited scope or the perspective from which it comes, can capture the entirety of a complex crisis. As such, cooperation between analysts from different sectors who use different methodologies is imperative to take advantage of potential synergies and fill information and methodological gaps. Representatives of these sectors and the military are encouraged to meet and sustain the current momentum toward comprehensive analysis. CCOE is willing to support this initiative in cooperation with partners.

Moving forward

The Comprehensive Analysis syndicate was an important first step towards civil-military cooperation in analysis. Many participants realised how difficult it is to look at large, complex questions with others from different backgrounds and viewpoints. However, this is in part what made this exercise valuable and worth continuing. Overcoming culture clashes, learning each other's' language and building trust requires a sustained practice of coming together and creating a dialogue. It is essential that leaders are made to understand the importance of this in order for challenges of over-classification and under-resourcing to be overcome and for a culture that sees analysis as a high priority. This move towards collaboration follows on from significant and pre-existing actions taken by stakeholders to improve analysis practices and outcomes. A key example is the United Nations Office for the Coordination of Humanitarian Affairs aim to build a better understanding of the challenges faced in humanitarian conflict analysis, and achieve more comprehensive analysis through two initiatives:

1. Breaking down silos in the Humanitarian Development Peacebuilding Nexus and improving collaboration among the key stakeholders, such as military actors, at the Humanitarian Networks and Partnerships Week, taking place in Geneva February 2019.

2. Establishing the Centre for Humanitarian Data in The Netherlands, which focuses on increasing the use and impact of data in the humanitarian sector, manages the Humanitarian Data Exchange, offers training and builds an active network that brings organizations together to work on data challenges collaboratively.

Furthermore, there is a cross-sector Conflict Analyst Network in Syria that is demonstrating possibilities for collaboration in the future. The CCOE, as demonstrated by this workshop, is bringing civilian and military actors together. This meeting of different sectors is an essential step forward for comprehensive analysis as organizational and cultural differences, and lack of trust between civilian and military sectors, whether real or perceived, hinders information sharing and collaboration. To achieve a solution for enabling comprehensive analysis, further targeted development work is recommended. This should occur in the near future to leverage the interest and momentum that has been generated. During the workshop, several suggestions were made for the next steps to take for the wider community interested in working towards comprehensive analysis:

1. Hold more narrowly-focused comprehensive analysis workshops in the future. Identify a key focal point or scenario for analysis across sectors and between the strategic, operational and tactical levels; the required output being a comprehensive analysis product, adding value to the holistic picture of complex environments and enhancing decision-making.

2. CIMIC Analysis training, and determining what good training would look like. Identified as a necessary next step to increase CIMIC analysis capacity and involvement.

3. Organise a case study for joint analysis. Enables discussion and exploration of how to integrate different analyses in a practical way.

4. On an individual level, self-evaluation. Necessary to be aware of personal and societal biases that may influence analysis. Both civilian and military actors highlighted throughout the workshop the negative impact this has on both information collection and the validity of analysis. Furthermore, genuine cooperation requires changing mind-sets from seeing other sectors as only a source of information to viewing them as partners in reaching common goals.

The syndicate raised many questions, rather than proposing solutions, that require further dialogue and input from a wider range of stakeholders than were present.

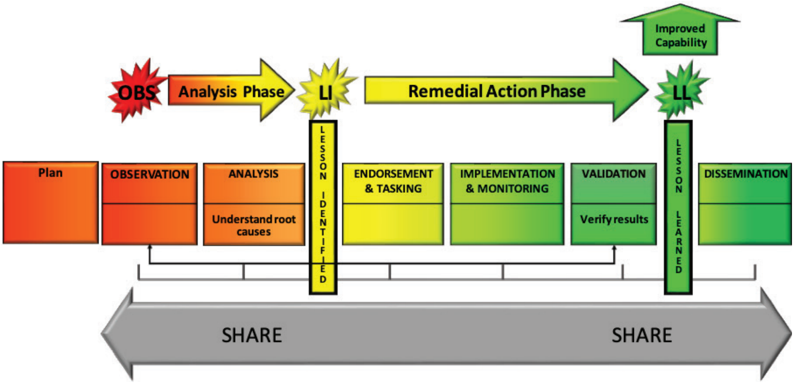
"For the strategic level you need to have an understanding of all the actors involved, how we work, a lot of relationship building, how do you establish a vision for what you want to do and find a way to strategically addressed that vision or those goals."

Mohan Ramesh Rajasingham
Director UN OCHA Coordination Division

ANALYSIS
Makes the Difference

Syndicate 2 - CIMIC Lessons Learned

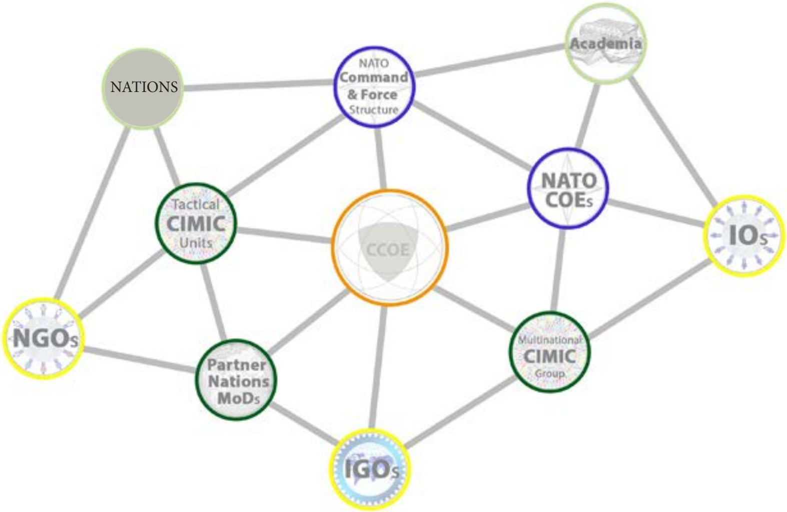
Continuous improvement occurs when individuals and organisations apply their experiences and practical knowledge to avoid repeating mistakes or help others avoid those same mistakes. Improvement also occurs when best practices are shared throughout an organisation or with other organisations. Learning from operations, training, exercises and other events enables continuous improvement. This capability of creating ongoing improvement through the sharing of experiences and practical knowledge is known as the Lessons Learned capability. It is a major driver for successful transformation. Lessons Learned should not be considered the final step of a process; the real value of lessons lie in their exploitation as inputs for better performance in current and future activities.



The Lessons Learned Process provides a structured framework to capture and pass on practical experiences and knowledge for the benefit of others. The observation is the trigger for the Lessons Learned process. The quality of the observation as the initial input into the process has a direct impact on the quality of the outcome. Those observations may be collected from reports, in daily staff work, exercises or missions. Experience shows, that Observations, Lessons Identified (LI), and Lessons Learned (LL) are often not shared widely, limiting the benefit for others.

Strengthen the CIMIC Lessons Learned Community

CCOE's intention is to build a CIMIC Lessons Learned Community and a common understanding of the lessons learned process. This seeks to also raise awareness for the value it has for CIMIC as a capability itself. Therefore the Lessons Learned training in Syndicate 2 aimed to ensure a high quality of observations as an input to the Lessons Learned cycle in order to receive viable Lessons Identified at the end of the process. The syndicate had two main objectives. Firstly, it was to conduct tailor-made training for CIMIC Lessons Learned personnel and interested civilians. Secondly, it was to conduct a kick-off event to strengthen the CIMIC Lessons Learned Community, with a special focus on the structures, tools, processes, and training.



CIMIC Lessons Learned Community

Tailor-made training

During the workshop, a three-day Lessons Learned Training was conducted by the Joint Analysis and Lessons Learned Centre (JALLC) Mobile Training Team. The idea of this training was to improve the skills and knowledge of the responsible persons for Lessons Learned in different units and organizations. In that sense, it had the following learning objectives:

1. Understand the management and execution of the various phases and steps of the NATO Lessons Learned process into the daily cycle of command, staff, and unit activities with the intent to improve current and future learning performance. NATO Mission Partners will have a better understanding of how to exchange lessons with NATO.

2. Know the key elements of the NATO Lessons Learned Capability, recognize and consider gaps in this context, and influence the direction of requirements to achieve improvement, especially in relation and support of the overall Lessons Learned process.

3. Analyze observations by applying various structured analysis techniques with the goal of discovering the root cause, suggesting conclusions, and supporting decision-making.

4. Describe and identify the handling of lessons in NATO exercises and operations in reference to given direction and guidance of the NATO policy, when operating as a partner with NATO forces.

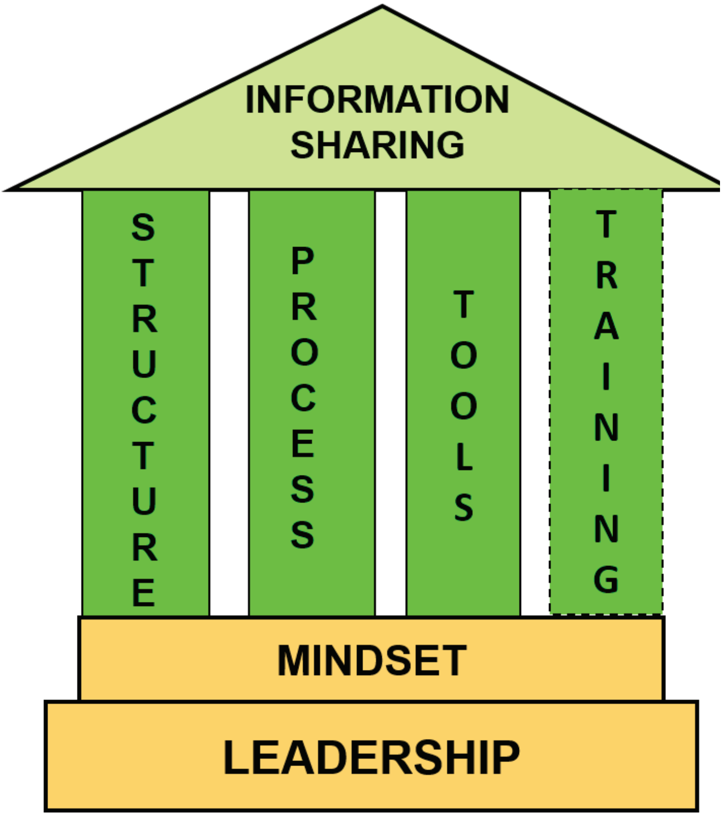
5. Understand the purpose of the NATO Lessons Learned Portal and it's handling in support of the Lessons Identified, Lessons Learned and Best Practice data management and Lessons Learned sharing.

> *"Lessons Learned & Analysis capability also demonstrates the excellence of a COE. It enables the COE to perform its own work more effectively and efficientely and enables it to a better support of NATO in his role as a learning organization."*
>
> John Varmark Jakobsen
> Branch Chief Lessons LL&A Branch CCOE

CIMIC Lessons Learned Community Kick-off

The aim of this subject was to enhance the CIMIC Lessons Learned collection and sharing tools, procedures and structures. This should be achieved in a first step by investigating the structures, tools, processes, and training that are in place throughout Organizations and Nations to collect and share CIMIC Lessons Learned. This intends to develop better how CIMIC Lessons Learned can be collected and shared and more effectively among organizations and partners. Furthermore, this subject offered the chance to discuss the possible role of the CCOE within the CIMIC specific LL process.

Therefore the workshop participants were asked to identify which structures, processes, tools, and training are supporting the development of a CIMIC Lessons Learned Community and which role this implies for the CCOE.



NATO Lessons Learnd Capability

Outcome and findings

The outcomes and findings are describing the role of the CCOE, according to the feedback of the workshop participants.

1. **Structure**

    a. Strengthen the military CIMIC Lessons Learned and involve the civilian Lessons Learned sphere in order to build a common CIMIC Lessons Learned Community.

    b. Identify the responsible persons for Lessons Learned in the CIMIC Community. Traditionally, the Lessons Learned role is, in most units and civilian organizations, an auxiliary function. The CCOE is in the lead to gather the players from the different units and organizations together.

    c. Use the already existing structure within NATO and the different organization's contacts to promote CIMIC Lessons Learned and change the mind-set of the leadership/key leaders. This can, for example, be done at conferences and courses.

2. **Process**
    Coordinate the collection plan for the CIMIC Lessons Learned Community.

3. **Tools**

    a. Be responsible for the CIMIC Lessons Learned contacts network list and update on a regular basis.

    b. Include the Lessons Learned process in the CCOE CIMIC Handbook.

    c. The CIMIC Lessons Learned Community should only use the existing portal, chatroom etc. provided by JALLC. The portal should also be accessible for civilian actors.

4. **Training**

    a. In cooperation with the JALLC, develop and provide Lessons Learned training for the Point of Contacts in the CIMIC Community and for interested civilian organizations.

Focus on training of Key Leaders/Leadership, which can be done for example with a lesson in CCOE's NATO CMI/ CIMIC Higher Command Course.

    b. Develop and provide a session that can be used to train the trainer in different CIMIC units or civilian organizations.

Moving forward

The Lessons Learned and Analysis Branch of the CCOE will take the outcomes as a starting point for building and developing the CIMIC Lessons Learned Community and include this as an integral part of CCOE's Lessons Learned and Analysis Branch program of work for 2019.

John Varmark Jakobsen, Branch Chief Lessons Learned & Analysis Branch CCOE

Syndicate 3 - Civil-Military Information Sharing

The current state of information sharing conventions in the military does not optimise the potential for an information-sharing environment with the civil sector. Natural disasters through to complex conflicts require cooperation between military and humanitarian actors to deliver a coordinated and effective response; timely and accurate information exchange is key to success. The military and civil actors must understand one another's objectives and, where appropriate, integrate information to minimise incongruences and promote harmony of effort. Stakeholders must seek best practice in Civil-Military information sharing, not only in conducting an immediate response but also in education, training, and preparation.

Syndicate 3 focused on improving the capabilities of military organizations to share information with civilians, and to manage and use information regarding the civil environment effectively, efficiently and appropriately. It was led by the Federated Mission Networking and Mission Partner Environment, Civilian-Military Information Sharing project team. This project aims to provide capabilities that support Civil-Military information sharing where this is critical to mission accomplishment, within the framework of the Federated Mission Networking construct. It is a project under the Multinational Capability Development Campaign of which NATO is a member.

Information sharing working group

The three-day discussion was conducted through a combination of briefings, reviews, and discussions in a working group format. Presentations from Humanitarian Data Exchange, Protection of Civilians, Netherlands Organization for Applied Scientific Research, and Marine Civil Information Management System (MARCIMS) enriched the discussions by contributing to deepening the knowledge on how information sharing from the civil side is performed and to identify the latest developments on the military side. The main subjects discussed were the following:

1. **How the current Civil-Military information sharing solution products are transferred to an organized community of practice.**
   a. Revision of the Federated Mission Networking and Mission Partner Environment current products by the participants;
   b. Discussion of ways to introduce concepts and practices;
   c. Recognizing the unique role of CCOE as CIMIC doctrinal custodian for NATO and as a hub for collaboration by the Civil-Military community;
   d. Identification of ways to sustain momentum and build a community of practice; and
   e. Proposal for a Civilian Information Management project to complement Federated Mission Networking and Mission Partner Environment, Civilian-Military Information Sharing.

2. How the lessons learned from the Federated Mission Networking and Mission Partner Environment project are to be applied by the Community of Interest to address the challenge of Civilian Information Management.

a. Reviewed current efforts which offer opportunities for transition and sustainment;

b. Reviewed challenges in maintaining multinational and Civil-Military cooperation; and

c. Developed a concept for a near-term Civil-Military Information project concepts for consideration by participants through the:

   i. Identification of problems and gaps in information collection, data management, and data sharing (i.e. MARCIMS and KOBOTOOLBOX);

   ii. From this determine a list of requirements based on user needs;

   iii. Engage with civilian and military-technical specialists to develop a common way ahead;

   iv. Using limited objective exercises, conduct a series of test and evaluation events to refine the solution and to validate and verify the tool with end users.

Outcome and findings

The community of interest and practice left the workshop with a shared vision and a common approach to solving common Civil-Military Information Capability challenges in a collaborative way.

Furthermore the discussions throughout the workshop pointed out, which preconditions for an effective Civil- Military Information Sharing needs to be met:

- The overall requirement are organizational and cultural shifts in order to cultivate trust among each other as a precondition for information sharing.
- Based on this trust relationship it requires the preparation of a legal framework that results in internal policies which allows information sharing.
- Within the context of those policies, doctrinal support from different actors is required as it delineates the processes and required outcomes of the information exchange.
- In order to allow an unhampered communication and exchange of data, it is necessary to create a common understanding based on the use of standard protocols and a common language including symbols, abbreviations etc. The Humanitarian Exchange Language (HXL) was discussed as a promising approach for a solution.
- In the same context it was stated that technicality, connectivity and interoperability should be improved in order to cut down or at least avoid further fragmentation
- The validity and reliability of data is a serious security concern related to the data itself, its source and the entire system. Corrupted data may have a negative impact on informational products in subsequent stages of information management processes.
- Any information sharing service needs to address ownership issues, as contributors wants to maintain access to their once provided data and also want to prevent misuse of it.
- In regard to accessibility and usability it was mentioned, that an easy to use Web platform based on open access (shared/cloud) is the most practical solution.

Workshop participants also identified issues that may foster or hamper Civil-Military Information Sharing. The previously mentioned requirements have indicate many relevant factors. In addition the participants offered significant insights:

- As mutual trust was identified as crucial, the following items have been pointed out as supportive to this requirement:
- Joint Exercises
- Common Training and courses
- Joint Analysis
- Common goal for a mission
- Existing relations between organizations
- Based on those relations, a Memorandum of Understanding on technical arrangements already in place facilitates CIV MIL information exchange.
- The usage of common tools and data i.e. for joint analysis eases the exchange of information.
- Information sharing requires a well-balanced and sensitive approach to handle the dichotomy between classification and privacy, as especially those factors have a significant impact on trust.
- The grade of difficulty to use the system is inverse to the willingness of users to operate with it. Therefore functionality out weighs complexity.
- Ultimately, constrains may arise from the conflict between those actors applying to the humanitarian principles and on the contrary, the security environment including military actors they are acting in. Those may also undermine an existing trust relationship.

In general there was broad consensus that finding a solution for an efficient way to share information between military and civil entities is more a question of mind-set and trust than technology. Deriving from this finding it was agreed, that further fragmentation of systems would be counterproductive. Standardization and the development of a system of system would ease Civil-Military Information Sharing instead.

As a consequence participants agreed that the following events are an adequate approach to build a community of practices in order to develop further trust and mind-set:

1. **Conferences**

   a. UNOCHA Regional Consultative Group on Humanitarian Civil-Military Coordination.

   b. Humanitarian Networks Partnerships Week (HNPW).

2. **Potential Exercises**

   a. Joint Cooperation.

   b. Trident Juncture.

   c. Viking Exercise (2021).

   d. RIMPAC – Humanitarian Response Phase (2020, 2022).

   e. Cobra Gold (annual).

Moving forward

CCOE will take the steps identified in the community of practice by:

1. Introducing the findings in information sharing lectures delivered in CCOE's training landscape;

2. Submitting findings in the Civil-Military Information Sharing chapter of CCOE's CIMIC Handbook and in CIMIC Doctrine;

3. Studying viability of a Civil-Military Information Sharing Workshop, in September 2019;

4. Supporting a Civil-Military Information Management project and serving as an information hub for the sharing of best practices and lessons learned across the community.

CCOE’s Way Ahead

This workshop was not intended as a standalone event; the CCOE seeks to reflect the outcomes of the ‘Analysis Makes the Difference’ workshop in the 2019 Program of Work to ensure continuity and sustainability.

The outcomes of **Syndicate 1** regarding Comprehensive Analysis encouraged the Department Head for CIMIC Training and Education to have a deeper look into this topic and its applicability to future programs. Therefore, CCOE intends to develop an in-house analysis capability to determine the impact on the CIMIC training landscape. Findings will be also reflected in the 5th Edition of the CCOE CIMIC Handbook, which will be promulgated in April 2019.

External contributions to these processes and products are necessary and welcome in order to create a comprehensive product. The Training Requirements Analysis in December 2018 and the Annual Discipline Conference in May 2019 provide opportunities to express training requirements and recommendations for this subject. CCOE is well-positioned and willing to support any relevant actors seeking to further this work through future workshops or case studies for joint analysis, enabling a more narrow focus on comprehensive analysis.

To work towards comprehensive analysis, future discussions should focus on answering following questions, which derived from the workshop discussions:

1. Do we take the civil-military approach seriously? Within this is a subset of key questions: What civilian and military actors are included? Do all stakeholders share the same understanding of comprehensive analysis? Are we looking as broadly as possible, or going back to default, established relationships with those we already know how to speak to (i.e. coalition forces)?

2. How can information-sharing relationships be established with all stakeholders in the conflict - including non-traditional partners such as Iran, Russia, and China?

3. How can the analytical community do more to influence strategic-level decision-making?

4. Are the correct questions being asked? How can analysts be enabled to drive the conversation around problem and question definition, rather than this being top-down from decision-makers?

5. What needs to happen to institutionalize information sharing to prevent the loss of progress at the end of four-month deployments?

6. How can we share information that is timely and avoids the constraints of over-classification?

Syndicate 2 showed the clear need for a CIMIC specific Lessons Learned Concept; CCOE's Lessons Learned and Analysis Branch is eager to develop and implement this in close cooperation with partners from the Lessons Learned Community and the CIMIC Community more broadly.

According to the workshop outcomes, CCOE Lessons Learned and Analysis Branch shall act as an intermediary with a facilitating role between those spheres. As this is a long-term process, it is our intention to implement the Lessons Learned Concept in the CIMIC Vision 2025, which will be finalised in May 2019. In preparation for this, CCOE Lessons Learned and Analysis Branch will develop a proposal for a CIMIC Lessons Learned Concept in the first quarter of 2019; discussing this with partners from national CIMIC units and CIMIC Lessons Learned POCs from NATO Command and Force Structure. In a second step (2019/2020), this concept shall be linked with interested non-military organizations, as it is inevitable to include civilian Lessons Learned capabilities to identify root causes from observations made in a Civil-Military environment. As the workshop showed that CCOE is an appropriate independent networking hub to discuss topics of mutual interest for the military and civil spheres, CCOE Lessons Learned and Analysis Branch will actively take the role of facilitator on this subject moving forward.

The results from **Syndicate 3** showed that Civil-Military Information Sharing must be an important focus of the CCOE's efforts in the upcoming year. In addition to implementing the findings of this workshop into the training landscape, it will also be reflected in the 5th Edition of the CCOE CIMIC Handbook. Furthermore, CCOE will explore this subject further within the established community of interest in order to stay up to date and reflect new developments in our products. Civil-Military Information Sharing will be a focus area for CCOE Lessons Learned and Analysis Branch to collect Observations, Lessons Identified, Lessons Learned and Best Practice in order to showcase the added value of the Lessons Learned Competence for CIMIC as a capability.

Participants Analysis Makes the Difference Workshop

CCOE

CCOE
CCOE

minorities as well as the rights of persons at risk o
displacement or already affected by it, need to be
effectively protected in all phases of the conflict cy
UNHCR
OSCE
CCOE
CIVIL-MILITARY COOPERATION CENTRE OF EXCELLENCE
THE HAGUE

CCOE

Ramesh Rajasingham
Director, Coordination Division UN OCHA
25 years of experience in the field of humanitarian affairs and with the United Nations.
Different assignments in Headquarters as well as in crisis settings and served as Deputy Humanitarian Coordinator for the Syria Crisis.
Interview by: LL&A, PAO CCOE

CCOE

One aspect of our workshop is actually, to examine the requirements from decision makers related to analysis:

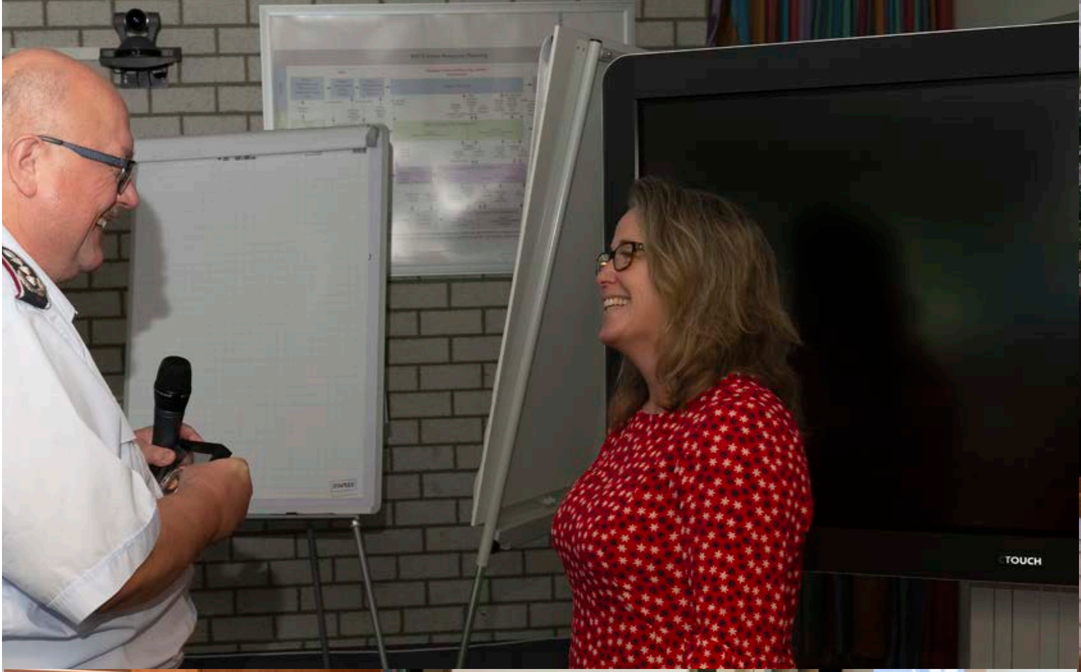
From your first-hand experiences as a decision maker;

What are the challenges in the analysis? Especially with regard to timeliness and confidentiality?

Method
What, Doctrine,
Where, CCOE
When, 2019,
How, NATO Standard Procedures,
Checklist
CCOE

Kim Vibring

CCOE


TOUCH

As you know of the World Humanitarian Summit there has b
spike in en und the Humanitarian – development and
peacebui ame time as the UN Secretary General has c
for a focu tion and resolution from all parts of the UN
What ad and pressure does this take place on the co
underst makers?

CCOE
CIVIL-MILITARY COOPERATION
CENTRE OF EXCELLENCE
THE HAGUE

RØDE
RØDE
Canon
Canon

UN OCHA
GENEVA
CISCO
Advanced Control

Illustrative Findings: Payinjiar (May 2017)
Actual perpetrators
SPLA, criminals and people from other communities were reported the most frequent perpetrators by respondents affected by security incidents
National army (SPLA)
Criminals
People from other community
Neighbourhood guard
People from own community
Clan family
Rebel group
Paramilitary forces
77%
70%
61%
41%
13%
2%
2%
1%
Potential future perpetrators
National army (SPLA)
People from other community
Unknown gunman
Neighborhood guard
Police
Rebel group/local armed group
People from this community
79%
26%
24%
22%
13%
9%
4%
SPLA also most frequently mentione
potential future perpetrator by respondents fearing incidents in the nex
NB: Multiple answers possible on both questions

MCD

CCOE

ANALYSIS
Makes the Difference
CCOE
CIVIL-MILITARY COOPERATION
CENTRE OF EXCELLENCE
THE HAGUE

CCOE
CIVIL-MILITARY COOPERATION
CENTRE OF EXCELLENCE
THE HAGUE
f
in
flickr
t

Illustrative Findings: Payinjiar (May 2017)
Actual perpetrators
SPLA, criminals and people from other communities were reported the most frequent perpetrators by respondents affected by security incidents
National army (SPLA)
Criminals
People from other community
Neighbourhood guard
People from own community
Own family
Rebel group
Paramilitary forces
77%
70%
61%
41%
13%
2%
2%
1%
Potential future perpetrators
79%
26%
24%
22%
Police
15%
9%
4%
SPLA also most frequently mentioned a potential future perpetrator by respondents fearing incidents in the next ye
www.cimic-coe.org

MCDC
What,
Doctrine,
Where,
CCOE
Checklist
CIVMIL – Information
www.cimic-coe.org

Appendix

CCOE FACT SHEETS

Read it

In the last years there is a swift visible on where conflicts will be fought, due to this military personnel has been confronted with a series of topics that has no direct link with military education or training. Nevertheless these topics if not addressed will hamper the military commanders in achieving a sustainable outcome. Topics like the “Cross Cutting Topics”, Protection of Civilians, Cultural property protection etc. or topics that are being used but don’t have a clear status yet, like Good Governance or Rule of Law.
Currently there is no advisor designated for many of these topics, most of the time the assessment and advisement will be done by the CMI and CIMIC branch (J9).

To help these CIMIC operators to get into these topics, the CCOE CIC branch have, in cooperation with many International organisations, come up with fact sheets.

These are mend to help CIMIC operators to get a quick insight into the topic, on what it is and what to do with it.

To make the academical more practical.

Scan the QR Code for all CCOE Fact Sheets.

Resilience

A CCOE Fact Sheet

What is Resilience?

Why Resilience?

What type of Resilience? Resilience for whom?

- Individual;
- Societal;
- State;
- Regional and Global Resilience.

From which threats?

- Natural disasters/hazards;
- Man-made disasters/hazards;
- Terrorism;
- Cyber;
- Hybrid threats.

What are the key organizations?

- NATO;
- EU;
- UN.

What is NATO’s approach to Resilience?

- Seven baseline requirements;
- NATO’s contribution to Resilience (CEPCI);
- Cyber Defense;
- Hybrid threats;
- Cooperation with EU;
- Cooperation with partner countries;
- Civil-military readiness.

What is Resilience?

Resilience is a comprehensive and relatively new concept that has received attention within many disciplines and fields. Resilience was first introduced within the field of ecology in the 1970's[1]. Afterwards, its use expanded to other disciplines, such as psychology, environment, organizational management and economics.

In the past decades, the resilience concept has entered a wide range of security discourses, and has been applied in fields such as disaster preparedness, counterterrorism, critical infrastructure, cybersecurity and many others.[2] Applied to many disciplines in a short time, the concept of resilience has become a solution to many challenges in security and governance.[3] It has been described as "a system's emergent response to emergencies"[4]. Resilience can be described as the capacity to withstand and recover from shocks, absorb damage, resume function as normal as quickly and efficiently as possible following extreme disturbances. A resilient system maintains stability and safety[5]; diminishes the possibility of failure; reduces consequences of disturbances and speeds up the recovery period.[6] It comprises both "Pre" -preparedness and "Post"- response to disturbances.

Why Resilience?

Today, we live in a complex security environment. The frequency and severity of threats continues to increase, and new threats and hazards are constantly emerging.

In the environment where the threats are complex and unpredictable, it is impossible to guarantee complete security. Current threats do not only impact human lives, but also economic and social development as well as security environment of states.

[1] Walker, J. and M. Cooper. 2011. Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. Security Dialogue. 42(2): 143-160

[2] Cavelty MD, Kaufmann M, Kristensen KS (2015) Resilience and (in) security: practices, subjects, temporalities. Security Dialogue 46(1): 3–14

[3] Aradau, C. (2014). The promise of security: resilience, surprise and epistemic politics. Resilience, 2(2): 73-87.

[4] M. Kaufmann (2016) Emergent self-organization in emergencies: resilience. Security Dialogue 47(2): 99 –116

[5] Cavelty MD, Kaufmann M, Kristensen KS (2015) Resilience and (in) security: practices, subjects, temporalities. Security Dialogue 46(1): 3–14

[6] Tierney, K. and Bruneau, M., (2007) Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. TR News 250: 14-17

This dynamic environment requires comprehensive precautionary measures. Simply reacting to a disaster or crisis is no longer seems sufficient; a more preventive approach is needed. Due to that, it is more effective to identify and address the root causes of threats than dealing with their consequences. The rehabilitation period of states and communities after the disasters and crises increasingly require more time and resources. In the long term, building resilience would be more effective, and with time, also cost-efficient.

Resilience can strengthen the capacity of individuals, communities, but also states towards disruptive events.[7] Even though complete protection from those events may sometimes not be feasible, resilience can help preparing to withstand those disturbances, and quickly recover from their effects.

What type of Resilience? Resilience for whom?

Considering the diversity of threats and their targets, resilience can be observed at different levels of society. All levels are interconnected and influence each other.

Individual resilience is demonstrated by the ability of individuals to withstand changes, adapt to and recover from traumatic events. Individuals may face shocks such as stress, social disorder, poverty, loss of family member or a job. Individuals with strong resilience are healthy, less susceptible to stress and have an ability, skills, and knowledge to cope with challenges and disturbances. Resilient individuals also participate in community resilient efforts, as well as contribute to the overall state resilience.[8]

Societal resilience is demonstrated by the capacity of community to prepare for hazards, diminish and prevent damages to people, property and environment, restore the basic services and function effectively in the aftermath of disturbances. A resilient community is self-mobilized, has an efficient and effective infrastructure and is able to respond to hazards by utilizing its own resources. Members of a resilient community are well connected, educated, and disaster-prepared.[9]

[7] Cavelty MD, Kaufmann M, Kristensen KS (2015) Resilience and (in) security: practices, subjects, temporalities. Security Dialogue 46(1): 3–14

[8] IFRC(2014) IFRC Framework for Community Resilience

[9] Norris FH1, Stevens SP, Pfefferbaum B, Wyche KF, Pfefferbaum RL.(2008) Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness, Am J Community Psychol, ;41(1-2):127-50.

State resilience is demonstrated by a "state's ability to withstand or recover from strategic shocks that stress and possibly distort state institutions and political settlements".[10] State resilience tackles the issues related to the rule of law, governance, infrastructure and social security systems. The hazards that pose challenges can be "internal or external, natural or orchestrated or as part of a hybrid attack".[11] In this respect, building and enhancing resilience requires collaboration between civilian, economic, private and military factors. By taking long term resilience measures, a nation state can diminish expenses, time and human lives connected to a threat, and return to the previous state of function without any major problems.[12]

Regional and global resilience is demonstrated by the ability of cooperating regionally or internationally to address regional or global hazards such as conflicts, disasters, climate change, hunger, mass migration, diseases as well as cyber and hybrid threats. A number of regional and international organizations are strengthening the capacity of regions and states with a range of programs and projects to help build resilience against future hazards.[13]

From which threats?

In today's world, we face an unprecedented range of security challenges. In order to combat those challenges, a simultaneous response to all hazards - both natural and man-made – would be required.[14] Natural disasters include earthquakes, hurricanes, tsunamis, wind storms, avalanches as well as epidemics, while man-made disaster can be complex emergencies/ conflicts, famine, displaced populations, industrial/transport accidents, terrorism, cyber, and hybrid threats. The most current and likely threats will be discussed below.

[10] CCOE (2017) A Civil-Military Response to Hybrid Threats to be published

[11] Ibid

[12] Ibid

[13] IFRC(2014) IFRC Framework for Community Resilience

[14] Dainty ARJ and Bosher LS (2008) Integrating resilience into construction practice. In: Bosher LS (ed.) Hazards and the Built Environment: Attaining Built-in Resilience. London: Taylor and Francis

Natural Disaster:

The impact of each disaster is immense, as disasters have a direct effect not only on individuals and communities (such as death toll and infrastructure damage), but also a continuous effect on the social and economic situation of the state and region. In the last decade, thousands of people lost their lives, millions have been injured, became homeless or displaced by disasters. Total economic lost is estimated to be $1.3 trillion.[15]

Even though the duration of a disaster usually does not exceed more than a couple of days, the consequences and destruction caused by that disaster may take considerably longer to remediate. Furthermore, due to several global factors, such as climate change, population growth, urban migration and shortage of natural resources, the frequency and magnitude of disasters are expected to increase in the upcoming years.[16]

Taking effective resilience measures to unforeseeable disasters has become one of the primary global concerns. Building and enhancing resilience can diminish the impact of disasters and the destruction that follows. Moreover, it prepares individuals, communities and states to cope with potential future disasters and to have the capacity to return to normal life after a disruptive event. Building disaster resilience involves measures, such as:

- strengthening disaster governance;
- creating awareness and disaster preparedness among the population;
- improving early warning systems;
- introducing disaster risk management policies and programs;
- enhancing international cooperation between actors;
- Identifying and reconstructing disaster prone infrastructure.[17]

[15] UNISDR (2015) Sendai Framework for Disaster Risk Reduction 2015 – 2030
[16] DFID (2011) Defining Disaster Resilience: What does it mean for DFID?
[17] UNISDR (2015) Sendai Framework for Disaster Risk Reduction 2015 – 2030

Man-made Disasters:

Terrorism

9/11 terrorist attacks marked a turning point for not only history of United States, but the whole world. Despite the fact that terrorism wasn't a new phenomenon, after 9/11 it became a pressing topic which required the introduction of new laws and policies for countering terrorism. Terrorism was no longer the problem of a single state. Because of it, 'national security' and 'international cooperation' became interconnected terms in order to fight international terrorism.[18]

Individuals, nationalist or religious groups can be involved in terror related activities for a variety of reasons, and come from various ideological backgrounds. The background of the terrorists shows that it is not only coming from abroad, but can also be homegrown as a cause of radicalization.[19] Terrorists can have political and social motivations, such as gaining political influence, obtaining global recognition, or affecting a country's economy and security infrastructure. Throughout history, terrorist groups have targeted politicians, police, public officials, and foreign embassy staff by using different methods, for example, assassination, hijacking, kidnaping and suicide bombing.[20] Today the victims of the terror attacks are civilians rather than military or political figures.

The consequences of terror attacks can vary from causalities to infrastructure damage and economic loss. Additionally, it disturbs and endangers the security system of the state as a whole. Terror attacks also create a sense of fear among the population that leads to a change in personal behavior like increased ethnocentrism and xenophobia.[21]

Building resilience against terrorism includes combating its root causes such as preventing radicalization, improving awareness of the population to security issues, promoting inclusivity and diversity of the society, enhancing the cooperation and dialogue between international actors.

[18] Rogers P. (2008) Terrorism. Security Studies: An introduction, Taylor & Francis Group

[19] Veldhuis T. & Staun J. (2009) Islamist Radicalisation: A Root Cause Model. The Hague: Netherlands Institute of International Relations Clingendael

[20] Rapoport, D. (2004) 'The Four Waves of Modern Terrorism', in A. Cronin and J. Ludes (ed) Attacking Terrorism: Elements of a Grand Strategy, Washington DC: Georgetown University Press, 46-73

[21] Huddy, L, Feldman, S, Capelos, T and Provost, C (2002) The consequences of terrorism: Disentangling the effects of personal and national threat, Political Psychology, 23 (3). pp. 485-509.

Hybrid threats

Contemporary conflicts are no longer classified as traditional or irregular. Today, the lines between war and peace, regular and irregular forces, combatant and non-combatant, physical and virtual are increasingly blurring.[22] Nowadays, enemy intentionally target the weak points of opposition by using both conventional and unconventional means such as terror, propaganda, separatist activities, and cyber-attacks in order to achieve their specific objectives. Hence, the emerging nature of contemporary conflicts became more complicated than only involving military power.

These threats that pose challenges to the contemporary security environment are called hybrid threats. "Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder".[23] Both state and non-state actors with or without state funding can be involved in conducting hybrid threats.

NATO identified hybrid threats as "multimodal, low intensity, lethal and non-lethal threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction."[24]

Although hybrid threats violate the law of armed conflict and international law, due to their complex and contemporary nature, hybrid threats are not regulated by any international legal framework. This makes countering hybrid threats a challenge.

The rise of hybrid threats does not indicate the end of traditional conflicts, however, it does require the comprehensive approach for countering and withstanding attacks by using all available economic, political, diplomatic, technological, as well as intelligence tools.[25]

[22] Hoffman F .G. (2007), Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, VA: Potomac Institute for Policy Studies, 8

[23] Ibid

[24] CCOE (2017) A Civil-Military Response to Hybrid Threats.

[25] Ibid.

Cyber threats[26]

In addition to conventional threats, nowadays cyber threats are growing in frequency, sophistication and scope, becoming increasingly more damaging. The actors engaged in cyber activities can vary from individuals to hacktivist groups, but also include government organizations. Using sophisticated and powerful IT techniques, these actors penetrate the computer networks of individuals, organizations, businesses as well as state agencies. The scope of coordination and complexity required for a cyber-operation is usually indicative of the actor involved. The larger and powerful supporters (sponsors) are behind the more complex and bigger operations. Those high-powered operations are most likely funded by state entities.

Cyber-attacks may have different motivations and goals. It can be used for espionage, sabotage related activities, infrastructure damage, financial gain as well as for reaching political goals. In general, the target of espionage and sabotage related cyber operations is confidential and sensitive information. Acquiring sensitive and secret information allows achieving strategic objectives against adversaries, and provides a clear advantage. In addition, it also benefits political and military goals of the opposition (adversaries). Cyber threats can take advantage of existing vulnerabilities and affect critical infrastructure, energy and transportation system. This can result in massive revenue loss and damage to economy and stability of a state.

Enhancing resilience against cyber threats requires identifying risk and threat landscape, keeping pace with rapidly changing technologies, engaging with countries, organizations as well as private cyber security sector, exchanging cyber defense related information with partners, introducing training and exercises in order respond to and adapt security challenges.

Which organizations are involved?

NATO

Resilience is not a new concept for NATO. It was introduced during the Cold War to reinforce and maintain the capability of nations to be resistant during war and crisis situations. However, in order to tackle rapidly emerging threats and improve NATO's deterrence and defense capabilities, the NATO Readiness Action Plan was introduced at the 2014 Wales Summit.

[26] Ibid.

Taking into consideration the threats and vulnerabilities, minimum standards for national resilience have been agreed.[27] Therefore, seven baseline requirements considered the most critical to NATO's collective defense tasks were introduced. During the Warsaw Summit of 2016, "Commitment to Enhance Resilience" was adopted by the Alliance.[28]

NATO's Civil Emergency Planning Committee (CEPC) is involved in resilient building activities. CEPC contributes to NATO's strategic objectives with civilian expertise and capabilities in various fields such as terrorism, humanitarian aid, and disaster response, critical infrastructure protection, cyber and hybrid threats.[29]

EU

In response to the needs of people with regards to their protection and improvement of livelihoods in current risk environment, European Union launches and funds several initiatives on sustainable development, disaster risk reduction, humanitarian assistance, climate change adaptation, and nutrition/food security.[30] Furthermore, due to rapidly increasing contemporary challenges posed by hybrid and cyber threats, EU expanded cooperation with NATO on enhancing resilience towards those threats.[31] The Directorate-General for European Civil Protection and Humanitarian Aid Operations of European Commission is the main contributor for maintaining and building resilience.[32]

UN

A number of entities of United Nations are involved in building and promoting resilience in various fields. This include resilience towards natural disasters (UNDP[33], FAO[34], ESCAP[35]), resilience of agriculture based livelihoods (FAO)[36], resilience of cities (UNISDR[37], UN-Habitat[38]), resilience in protract-

[27] Available at: http://www.nato.int/cps/on/natohq/topics_119353.htm

[28] Available at: http://www.nato.int/cps/eu/natohq/official_texts_133180.htm?selectedLocale=en

[29] Available at: http://www.nato.int/cps/on/natohq/topics_50093.htm

[30] EU(2016) Building Resilience: The EU's approach Factsheet

[31] NATO (2017): NATO - EU Relations – Fact Sheet

[32] Available at: http://ec.europa.eu/echo/what/humanitarian-aid/resilience_en

[33] Available at: http://www.undp.org/content/undp/en/home/climate-and-disaster-resilience/disaster-risk-reduction.html

[34] Available at: http://www.fao.org/resilience/areas-of-work/natural-hazards/en/

[35] Available at: http://www.unescap.org/our-work/ict-disaster-risk-reduction

[36] FAO (2016) Increasing resilience of agriculture based livelihoods

[37] Available at: https://unhabitat.org/urban-themes/resilience/

[38] Available at: https://www.unisdr.org/we/campaign/cities

ed crisis (FAO)[39], conflict prevention and peacebuilding (UNDP)[40], climate resilience (UN Secretary General's climate resilience initiative (A2R)[41] and many other short and long term initiatives.

What is NATO's approach to Resilience?

Seven baseline requirements;

- Assured continuity of government and critical government services;
- Resilient energy supplies;
- Ability to deal effectively with the uncontrolled movement of people;
- Resilient food and water resources;
- Ability to deal with mass casualties;
- Resilient communications systems;
- Resilient transportation systems.[42]

NATOs´ approach on cyber-defense

In order to combat cyber threats it is noteworthy that NATO now recognizes cyber-space as a domain of operations as where they have to be as capable and effective as they are during air, sea and land operations. In pursuance of the prearranged aims NATO has released several projects and procedures to improve the allied cyber defense and to approach future cyber threats.

During the Wales summit in 2014 NATO members have agreed on passing a policy and action plan. This plan includes measures in order to establish and reinforce capabilities for cyber education and training. Furthermore, it enhances the information exchange between member countries and countries that might not be a part of NATO. Due to the asymmetric effects of cyber threats, the policy and action plan also comprehends internationally valid laws which are applying in cyber-space. On behalf of cyber defense, all member states have affirmed this law and included it into their national statutes.[43]

[39] Available at: http://www.fao.org/resilience/resources/protracted-crisis/en/

[40] Available at: http://www.undp.org/content/undp/en/home/ourwork/democratic-governance-and-peacebuilding/conflict-prevention-and-peacebuilding.html

[41] Available at: http://www.a2rinitiative.org/

[42] Available at: http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

[43] NATO (2017): Cyber defense, Online on the internet: URL: http://www.nato.int/cps/en/

Another aspect is the integration of cyber-defense into NATO´s smart defense initiative. Hereby member states contribute resources and knowledge to form a joint task force. Especially the research and development department is in need of a lot of resources which most likely cannot be handled by a single country. Additionally, NATO has established a trust fund for cyber defense which can be used to finance the necessary activities and programs. Nameable projects are for example the Malware Information Platform (MISP) or the Multinational Cyber Defense Crisis Management Exercise (MN CD2).[44]

Because of the crucial prominence of the private IT-sector NATO has also started to cooperate with globally acting companies. By foundation of cross-sectional and multinational Smart Defense Projects, cooperating with private companies, both sides can profit from each other. Main goal is the exchange of expertise and technological innovations from either the military or private sector.[45]

NATOs´ approach to hybrid threats

NATO issued the Lisbon Summit Declaration in 2010, in which it explains how NATO is planning on tackling hybrid threats. Main aim is to defend its members against the full range of threats and to promote international stability. To stay effective over a long-term period, NATO members decided to operate more agile, cost-effective and to serve as an essential instrument for peace.

In pursuance of those goals, NATO is required to closer cooperate with political or military organizations such as the European Union or the United Nations. Besides working with allied countries it is also beneficial to deepen the relationship with non-allied but still influential powers like Russia. This cooperation might involve the exchange of inventories or information.[46]

NATO members agreed on developing new high-tech weapons systems (e.g. missile-defense), in the interest of protecting Allied countries against foreign or domestic attacks.

natohq/topics_78170.html.

[44] Stoltenberg, J. (2017): Press conference ahead of the meeting of NATO Defense Ministers, Online on the Internet: URL: http://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en.

[45] NATO (2017): NATO Policy on Cyber Defense, Online on the Internet: URL: http://www.nato.int/cps/en/natohq/topics_78170.html.

[46] Bachmann, S. (2012): Hybrid threats, cyber warfare and NATO´s comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management; in: Amicus curiae, Vol. 8, 2012, P. 14-17.

With regard to not act aggressively towards surrounding countries, NATO officials have invited Russia to join the development process and planning.[47] Beneficial to a successful long-term functionality it is also essential to enhance existing partner relationships and to develop and negotiate new ones with interested partners.[48]

Cooperation with partner countries

In the interest of resilience NATO has to go beyond the usual work within member countries. It is also important to establish long-term associations with neighboring countries or even partners from all around the globe. Therefore, NATO has introduced several cooperating relationships which can contribute to fulfill the main goals, defined by the United Nations Security Council Resolution. These goals involve the protection and improvement of women rights, boarder defense and combating human traffic plus terrorism.

NATO has tight relations to the Euro-Atlantic-Partners (EAPC), which is a group of 29 Allies but also 21 non-member countries. Main task here is the consultation about political and security related issues, which include crisis management and peace supporting operations.[49]

Furthermore, NATO came up with the Mediterranean Dialogue Program, which was initiated in 1994. Hereby the 29 member states get the chance to step into contact with ambassadors of seven North-African states. Each state has the chance to consult collectively or individually with NATO in order to contribute to regional security and stability, to achieve improved mutual understanding and finally to dispel misconceptions about NATO among Mediterranean nations.[50]

While most current conflicts are located in the Middle East, NATO started the Istanbul Cooperation Initiative (ICI). The main reason behind it was to establish a security cooperation with such nations from the Middle East. It turned out to be a very helpful source contributing to regional and global security.[51]

[47] NATO (2010): Lisbon Summit Declaration

[48] Ibid.

[49] NATO (2017): Euro-Atlantic Partnership Council, Online on the Internet: URL: http://www.nato.int/cps/de/natohq/topics_49276.htm

[50] NATO (2017): NATO Mediterranean Dialogue, Online on the Internet: URL: http://www.nato.int/cps/en/natohq/topics_60021.htm?

[51] NATO (2017): Relations with partners across the globe, Online on the Internet: URL: http://www.nato.int/cps/cs/natohq/topics_49188.htm?selectedLocale=en

Since security challenges are issues all around the world, NATO also tries to cooperate with partners around the globe. Therefore, they have established bilateral relations with countries who are not NATO or EAPC members.
In most cases those partners support NATO missions in either a military or civil way.[52] [53]

NATOs´ cooperation with the EU

The European Union and NATO are strategic partners. They cooperate on a wide variety of issues, including crisis management, capability development, building the capacities of partners, addressing hybrid threats and maritime security.[54] [55]

In July 2016, NATO and the EU expanded their relationship. As a result, a Joint Declaration was signed to boost cooperation in key, including countering hybrid and cyber threats, supporting partners in defense capacity building, improving information-sharing and cooperation in the Mediterranean Sea, as well as on defense capabilities, the defense industry and research, and exercises.

Following this a package of measures for the implementation of the Joint Declaration was presented in December 2016. These measures are now being implemented. They include: Measures to bolster resilience to hybrid threats, ranging from disinformation campaigns to acute crises, Enhanced cooperation between NATO's Operation Sea Guardian and the EUNAVFOR Operation Sophia in the Mediterranean Sea, exchange of information on cyber threats and the sharing of best practices on cyber security. Ensuring the coherence and complementarities of each other's defense planning processes as well as parallel and coordinated exercises, starting with a pilot project in 2017.[56] [57]

[52] NATO (2017): NATO member and partner countries, Online on the Internet: URL: http://www.nato.int/cps/is/natohq/topics_81136.htm

[53] NATO (2015): PARTNERS, Online on the Internet: URL: http://www.nato.int/cps/cs/natohq/51288.htm

[54] Đajić, O. (2015): The state of play of the EU – NATO partnership, Online on the Internet: URL: http://www.europeanleadershipnetwork.org/the-state-of-play-of-the-eunato-partnership_3076.html

[55] NATO (2017): NATO - EU Relations – Fact Sheet, Online on the Internet: URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170213_1702-factsheet-nato-eu-en.pdf

[56] Ibid

[57] Pop, A. (2007): NATO and the European Union: Cooperation and security, Online on the Internet: URL: http://www.nato.int/docu/review/2007/Partnerships_Old_New/NATO_EU_cooperation_security/EN/index.htm

Close cooperation between NATO and the EU is an important element in the development of an international “Comprehensive Approach” to crisis management and operations but not new. NATO and the EU cooperate for years on crisis management and operations, in particular in the Western Balkans and Afghanistan. NATO and the EU worked and still work together in Bosnia and Herzegovina (SFOR/Operation EUFOR Althea), Kosovo (KFOR/EULEX), Afghanistan (ISAF/EUPOL), Coast of Somalia (Operation Ocean Shield/EUNAVFOR Atalanta), during the refugee crisis and in many more cases.[58]

NATOs´ approach on civil-military readiness

NATO approaches civil-military readiness with its Readiness Action Plan (RAP) which was approved at the NATO Wales Summit in 2014. The RAP ensures that the Alliance is ready to respond swiftly and firmly to new security challenges. Due to that NATO members have to adjust their territorial defense mechanisms and infrastructure to the new security environment. This includes cross-border transit arrangements for the rapid deployments and the planning of transport, flight corridors, civil-military airspace coordination, fuel stocks, pre-positioned equipment, port access and legal agreements. Furthermore, the Allies have to update crisis-response, civil emergency and civil defense measures. These measures are the most significant reinforcement of NATO’s collective defense since the end of the Cold War.[59]

Assurance measures - NATO’s assurance measures are land, sea and air activities in and around NATO’s territory, especially the eastern flank for reinforcing NATO’s defense, reassuring civilians and deter aggressions. These measures are consequences of Russia’s aggressive acts in the past. All Allies support these measures rotationally. The measures are flexible and annually reviewed by the North Atlantic Council. Examples for assurance measures are air-policing patrols, AWACS surveillance flights, maritime patrol aircraft flights, a Standing NATO Mine Counter-Measures Group and an enlarged Standing NATO Maritime Group. Furthermore, NATO has increased the number of exercises on land, at sea and in the air which improves the ability of Allies and partners to work together and is a demonstration of NATO’s readiness and strength.[60]

[58] NATO (2017): NATO - EU Relations – Fact Sheet, Online on the Internet: URL: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170213_1702-factsheet-nato-eu-en.pdf

[59] Shea, J. (2016): Resilience: a core element of collective defense, Online on the Internet: URL: http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

[60] NATO (2016): NATO’s Readiness Action Plan – Fact Sheet, Online on the Internet: URL: http://nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf.

Adaption measures - Adaption measures are long-term changes to allow the Alliance to react swiftly and decisively to sudden crises which include the tripling of NRF's strength, the creation of a Very high readiness Joint task Force (VJTF), the establishing of high-readiness multinational headquarters and enhancing Standing Naval Forces.

Enhanced NATO Response Force (NRF) - The NRF is a highly ready multinational force of land, air, maritime and Special Operation Forces (SOF) components. The NRF is quickly deployable. In 2014 the Allied countries decided, that the NRF should be enhanced to strengthen the collective defense. Since then the NRF has a size of approx. 40,000 personnel which is much larger than the old size of 13,000.

Very High Readiness Joint Task Force (VJTF) - The VJTF, also called NATO's "spearhead force" has a size of approx. 20,000, of which about 5,000 are ground troops and is deployable within two or three days. The VJTF is supported by maritime and air components as well as SOF. VJTF forces are based in their home countries and will be deployed if needed. The command and membership of VJTF rotate every year.

NATO Force Integration Units (NFIUs) - NFIUs are small HQs which enable the deployment of the VJTF and other forces. They consist out of about 40 national and multinational NATO specialists. The task of the NFIUs is the improvement of the cooperation and coordination between NATO and national forces as well as to support and prepare exercises and deployments.[61]

Ibid

Disaster Relief

A CCOE Fact Sheet

Introduction:

This factsheet deals with the provision of relief operations during the rapid onset of disasters and the role of CIMIC officer in these operations.

> *"A disaster is a sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic or environmental losses that exceed the community's or society's ability to cope using its own resources."*[1]

A disaster can be man-made, or natural. Man-made disasters include complex emergencies/conflicts, famine, displaced populations, industrial accidents and transport accidents. Natural disasters include slow onset disasters such as crop failure, drought, the spread of an agricultural pest, or disease and the rapid onset disasters such as earthquakes, hurricanes, tsunamis, landslides, volcanic eruptions, wind storms, wild fires, typhoons, floods, and avalanches.

The affected state has the primary responsibility to respond to natural disasters within its territory. However, if the magnitude of the disaster exceeds capability of the affected state, the international community can provide disaster relief assistance.

> *"Disaster relief is the organized response to render assistance to those affected by a disaster. It requires rapid reaction and often includes services and transportation, rescue and evacuation of victims, the provision of food, clothing, medicine and medical services, temporary shelter, technical assistance, and repairs to essential services."*[2]

[1] www.ifrc.org/en/what-we-do/disaster-management/about-disasters/what-is-a-disaster/

[2] A.J.P-3.4.3

Mission Implications

1. In most cases, natural disasters can have cascading effects. Therefore, it is important to identify the historic frequency and magnitude of disasters which previously occurred in an area of operations in order to be better prepared for potential disasters during a particular mission. Besides cascading effects, factors like the weather condition, existence of any diseases and toxic animals need to be taking into account.

2. Confusion over the military's role and presence as in relief operations can lead to suspicion and fear among the affected population due to fact that non-state armed groups could take advantage of the disaster by violating local rules and regulations. This may create mistrust from the affected popu- lation towards state and NATO military in the area affected by disaster. As a result, some people may not benefit from the provided relief. In this respect, gaining local population's trust and acceptance is possible by constant communications and respect for local culture and traditions.

3. It is important to be aware of the effect that massive human casualities may have on mission troops operating in an affected area. This effect might lead to psychological problems of troops and may affect the mission. Therefore, provision of pre-/post deployment psychological assistance should be taking into consideration.

Leading Organizations:

1. **Within NATO**

Euro-Atlantic Disaster Response Coordination Centre (EADRCC) and the Euro Atlantic Disaster Response Unit (EADRU) are basic elements of the Euro-Atlantic Disaster Response Capability which contributes and supports UN entities during disaster relief operations.

EADRCC was established at NATO Headquarters in order to conduct disaster relief operations in the Euro-Atlantic Partnership Council geographic area.

Volunteered by EAPC countries, the EADRU is a non-standing, multinational organization, consisting of national civil and military elements such as qualified personnel for rescue, medical, and other entities; equipment and materials; assets and transport. The EADRU can be stationed in support for international organization during disaster relief operations upon the request of the affected state.

2. Within UN

A number of UN entities, funds and programs are directly and indirectly specialized in humanitarian assistance and disaster relief operations. These include the Office for the Coordination of Humanitarian Affairs (UN OCHA), World Food Program (WFP), the UN high Commissioner for the Refugees (UNHRC), the UN Children's Fund (UNICEF), World Health Organization (WHO), and the UN Development Program (UNDP) as well as many others. The lead agency during disaster response operations is UN OCHA, which is responsible for mobilization and coordination of international humanitarian assistance.

3. Within EU

European Civil Protection and Humanitarian Aid Operations (ECHO) is responsible for rapid and effective delivery of EU relief assistance in response to natural disasters. ECHO possess 48 field offices in over 40 countries, which enables it to acquire the latest information on the needs in a disaster affected region.

References:

- AJP-3.4.3 Allied Joint Doctrine for the Military Contribution to Humanitarian Assistance
- AJP 3.4.2 Allied Joint Doctrine for Non-combatant evacuation Operations
- CCOE CIMIC/CMI Field Handbook
- UN-CMCoord Field Handbook
- UN- CMCoord Guide for military

The “Do’s” and “Don’ts”:

Do’s

- Military activities within disaster relief are always under civilian control.
- Clarify if direct assistance is foreseen by humanitarian actors; carefully consider indirect assistance and infrastructure support (unless your mission include direct assistance).
- Conduct joint civil-military assessments in order to support ade quate planning and execution.
- Respect the culture, customs and gender related issues while providing relief operations.
- Avoid cultural mistakes in relation to the affected state’s traditions.
- Include woman CIMIC officers in relief efforts.
- Understand the mandates of the present relief actors.
- Respect the code of conduct and humanitarian principles.
- Make sure information exchange takes place between IOs/NGOs and the military.
- Consider the information you are allowed to share with humanitarian actors and be aware that not all the information will be shared with you.
- Constantly liaise with the population and create trust and acceptance.
- Follow the “do no harm” principles.
- Participate in cluster meetings if you are invited.

Don’ts

- Do not make promises you can’t keep to local authorities or affected population.
- Do not evaluate humanitarian personnel by their age and ranks. Age, ranks and hierarchies are less important in humanitarian organizations.
- Do not assume western personnel are the decision makers.
- Avoid duplication activities of humanitarian actors.
- Do not take the leading role. Lead only if requested by the affected state or the leading IO.
- Do not endanger the Military mission by over extending the support within Disaster Relief.

> *“Coordination between civilian and military actors is essential during an emergency response. The increasing number and scale of humanitarian emergencies, in both natural disasters and conflict settings, has led to more situations where military forces and civilian relief agencies are operating in the same environment.”*

John Holmes, Emergency Relief Coordinator and
UN Under-Secretary General for Humanitarian Affairs

CIMIC Tasks:

- Establish and maintain liaison with the affected state, civil population, IOs and NGOs.
- Enable effective and consistent information sharing concerning disaster relief within the mission area as well as affected state, IOs and NGOs.
- Engage in dialogue with the affected state or/and UN OCHA regarding their expectations of the military's role and responsibilities.
- Analyze the impact a disaster has on the missions role.
- Asses possible military contribution in support of a Disaster relief operation.
- Learn about role and responsibilities of other actors with regards to disaster relief.
- Develop an exit and transition to civilian ownership strategy as early as possible.

Upon request only/ be prepared to

- Act as an intermediate between humanitarian actors and the military.
- Assist civil actors in the effective distribution of humanitarian aid within means and capabilities of CIMIC.
- Restore infrastructure and essential services and clear main supply roads.
- Provide safety and evacuation services for affected population.
- Provide security/protection for humanitarian actors.
- Assist dislocated civilians with the support for camp organization, basic construction and administration provision of care and placement.

Cross-Cutting Topics:

Disaster relief has several overlapping concepts: It links to the Protection of Civilians in the context of natural disasters. Natural disasters can cause and worsen protection risks for civilians, such as enhance discrimination and lead to unequal access to humanitarian assistance; family separation; enforced relocation and issues and disputes related to land and property rights.

The disaster situation can also result in sexual and gender-based violence and child trafficking. In this matter, disaster relief also links to Gender and CAAC, because it also deals with the protection of men, women, boys and girls.

Additionally, Cultural Property Protection is also one of the cross cutting issues as it is important not to harm any "movable or immovable cultural property" of the affected state during the relief efforts. Rule of Law and Good Governance are very important, the perception that the affected nation is in lead and respects as International human rights law as well as national and local laws will have a great impact on the perception the local population will have on their trust in their own government.

Responsibilities in CMI:

Outside of J9 the different branches have the following responsibilities:

- J2 provides comprehensive analysis of the affected state including security aspects of the potential NATO disaster relief mission;
- J3 provides "mil to mil" coordination assets (it is important for the NATO CIMIC specialists to know the national CIMIC focal points);
- J4 provides capabilities including medical and military engineering dedicated for the disaster relief mission;
- J5 includes all CIMIC considerations into the disaster relief CONOP and OPLAN;
- J6 provides the capabilities and assures all CIS aspects of the operation including the necessary assets for the CIMIC;
- J7 provides disaster relief specialized pre-deployment training;
- J8 assures all financial aspects of the disaster relief operation;
- LEGAD provides advice on IDRL.

Legal Implications:

There are no legally binding regulations directly related to natural disasters, although there are some universal regulations which are applicable to natural disasters:

- "Universal Declaration of Human Rights (UDHR)" Although not legally binding, this declaration defines key concepts such as fundamental freedoms and human rights, forming the foundation for other binding treaties, legislation and regulations with respect to fundamental human rights.
- "International Human Rights Law" Following the introduction of the UDHR, a set of legally binding treaties were developed in order to further define the "obligations and duties of states to respect, protect and fulfill human rights".
- In addition to the aforementioned regulations, there are a number of non-binding regulations and guidelines which specifically address natural disasters. These include:
- International disaster response laws, rules and principles (IDRL guidelines) aims to improve disaster laws of states and non-state actors with regards to incoming international relief in the context of natural disasters.
- The Guidelines on the "Use of Foreign Military and Civil Defense Assets in Disaster Relief" (Oslo Guidelines) aim to provide a frame work for the use of military and civil defense forces in international disaster relief operations. NATO-led forces, as an EADRCC (Euro-Atlantic Disaster Response Coordination Center) asset may be requested to assist in disaster relief in accordance with the Oslo Guidelines, but only if no comparable civilian alternative is available.

Additionally, the legal status of military personnel during relief operations is established under the NATO Status of Forces Agreement (SOFA). However, military assistance during relief operations is constrained by the laws of NATO members and participating partner nations. It is also important to be aware of national and local laws of the affected country.

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.”

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

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

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.

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

Related topics:

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 de fence 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 care fully (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.

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.

NATO Civil-Military Interaction (CMI)

A CCOE Fact Sheet

Introduction:

NATO CMI can be seen as the primary means for military forces to both expand their knowledge networks and develop shared situational understanding of the civil environment with other relevant actors in the area of operations. CMI enables the necessary engagement and coordination process required to create, build and maintain relationships between relevant non-military and military actors. Within these relationships and engagements with non-military actors, the military must be regarded as an equal player.

With regard to facilitating NATO CMI, Civil-Military Cooperation (CIMIC) staff play a vital role. CIMIC interacts with non-military actors and thereby enables and facilitates CMI for other headquarters staff. CIMIC personnel are trained in bringing together the appropriate military and non-military actors. Facilitating CMI will differ at each level of command due to the focus, responsibilities and scope of coordination.

The introduction above leads to the following definition of NATO CMI:

> *"Civil-Military Interaction is a group of activities, founded on communication, planning and coordination, that all NATO military bodies share and conduct with international and local non-military actors, both during NATO operations and in preparation for them, which mutually increases the effectiveness and efficiency of their respective actions in responses to crises."*

Civil-Military Cooperation
Centre of Excellence

Mission Implications:

Recent operations have proved that crises cannot be resolved in isolation. Therefore, NATO is convinced that crises can best be managed by coordinating efforts with non-military actors. Properly established and maintained relationships between military and non-military actors lead to better understanding, the avoidance of possible conflicts as well as more effective and efficient actions to counter crisis situations.

Everyone within the mission needs to consider CMI to a certain extent. Especially those who have relations with non-military actors carry the responsibility to make an effort to first understand their non-military counterparts and second seek to be understood by them. In order to do this, the military must assess relevant information and utilize already existing knowledge on non-military actors. Next to this, the military must build new and explore and exploit existing networks within the civil environment prior to the mission. This in order to create relationships and build rapport with non-military actors they have to work side-by-side with and avoid having to start from scratch when the mission begins.

Relation NATO CMI and UN CMCOORD:

As mentioned above, NATO CMI is conducted between military and non-military actors within an area of operations, with the goal to increase effectiveness and efficiency of their responsive actions. In a lot of missions, NATO will have to work side by side with the UN and its organizations.

The UN uses a concept different from CMI, namely United Nations Humanitarian Civil-Military Coordination (UN-CMCoord). This concept is focused on interaction between non-military and military actors in humanitarian emergencies. The aim of this interaction should be to protect and promote humanitarian principles, avoid competition, minimize inconsistency, and, when appropriate, pursue common goals. Both concepts are aimed at developing a working relationship between military and non-military actors. This relationship differs in every situation. However, NATO CMI applies to every NATO mission and aims at the improved efficiency of both military and non-military actors, whereas the UN-CMCoord concept only applies to humanitarian missions and its sole purpose is the benefit of the humanitarian effort.

Assessment Implications:

Assessments help to create understanding with regard to the civil environment and non-military actors, and understand what consequences military actions can have on them within the area of operations. With regard to the assessments, CIMIC personnel plays a vital role. By using the PMESII (Political, Military, Economic, Social, Information and Infrastructure) and ASCOPE (Area, Structures, Capabilities, Organizations, People and Events) models CIMIC personnel can identify the best possible way to engage with non-military actors in a coherent and efficient manner.

Leading Organizations:

As mentioned, NATO CMI is the responsibility of all actors involved in crisis management in the area of operations. However, within the military the J9 branch has the responsibility to conduct assessments with regard to non-military actors, facilitate interaction between military and non-military actors and ensure a coherent military message.

CMI Principles:

The following principles should be taken into account when conducting CMI:

- Understand non-military actors and respect their autonomy in decision-making.
- Engage proactively with all non-military actors involved in the operation. Commanders in particular must maintain continuous and effective communication with their correspondent counterparts at local, regional, national and international levels.
- Facilitate interactions based upon mutual respect, knowledge of respective roles, trust and transparency. Institutional familiarity, credibility and reliability are key.
- Be able to adapt to evolving and specialized non-military expert advice and factors.
- Promote local ownership and build local capacity, ensuring timely and smooth transition to local ownership as soon as practical.
- Ensure internal NATO military coherence and consistent NATO messaging in interacting with non-military actors.
- Develop and implement a transition plan from the outset to

ensure transition to civilian ownership as early as possible when taking on non-military tasks.

- Promote cooperation, reciprocal information sharing and unity of purpose as a desired method to achieve overall strategic aims and objectives.
- Operate within the framework of the NATO mission, responsibilities, authorities and legal obligations.

Subjects for CMI:

Within the field of CMI, a number of important subjects can be identified that need to be discussed with non-military actors:

- Protection of Civilians
- Women, Peace and Security
- Cultural Property Protection
- Rule of Law
- Children and Armed Conflict
- Good Governance
- Building Integrity
- Gender

Point of Contact during the Mission:

Military actors should liaise with non-military actors in the area of operations such as Doctors without Borders, UNOCHA, UNDP, the local municipality etc.

Sources of Additional Information:

An example of the assessment of non-military actors in Afghanistan:

- https://www.cimic-coe.org/products/conceptual-design/downloads/ccoe-publications/research/

More information on UNCMCoord can be found here:

- https://www.unocha.org/sites/dms/Documents/CMCoord%20Field%20Handbook%20v1.0.pdf

More information on UNCMCoord from a military perspective here:

- https://www.unocha.org/sites/dms/Documents/UN%20OCHA%20Guide%20for%20the%20Military%20v%201.0.pdf

References:

- Civil-Military Cooperation Centre of Excellence (2014), Conceptual Considerations on Civil-Military Interaction
- MC 0411/2, NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMI)
- AJP-3.19, Allied Joint Doctrine for Civil-Military Cooperation
- Civil-Military Cooperation Centre of Excellence (2014), Best & Bad Practices on Civil-Military Interaction

Do’s and Don’ts:

Do’s

- Try to build (personal) relationships.
- Align relevant strategies in the planning phase.
- Evaluate and monitor your activities (and share the results).
- Share/communicate your way of operating.
- Describe the sustainability of your efforts.
- Respect each other’s decisions and try to deal with them.
- Communicate your time frame.

Don’ts

- Do not stereotype.
- Do not create barriers between military and non-military actors.
- Be careful not to disrespect each other’s principles.
- Do not create dependency.
- Avoid making promises you cannot keep, they will turn against you.
- Never underestimate the ‘need to share’.
- Do not plan in splendid isolation.
- Use existing structures and avoid creating new, parallel ones.

Children And Armed Conflict (CAAC)

A CCOE Fact Sheet

Introduction:

Children are involved in and affected by conflict in different ways, they are always victims and need to be protected, even when they may be perpetrators of crimes.

> *"In order to advance the goal of protecting children during armed conflict and ending the impunity of perpetrators, the United Nations Security Council identified six categories of violations – the so-called six grave violations, and are the basis of evidence-gathering. These violations are: Killing and maiming of children; Abduction of children; Recruitment or use of children; Rape or other grave Sexual violence; Attacks on schools and hospitals; Denial of humanitarian access."*

The violations are not ranked on importance, some of the violations will have more direct impacted on, depending on the environment, the mission. CIMIC personnel and Commanders need to be aware of these violations IOT mitigate any negative outcome towards the mission.

Mission Implications

Apart from the legal implications noted below, CAAC can also affect the Commander's mission more directly.

It can be mentally difficult or even damaging for armed forces to face child soldiers. It can also have demoralizing effects. When the CIMIC officer suspects their present in his AOR, the Commander needs to be notified, so that the proper education and psychological support can be provided. Soldiers should also be prepared on how to deal with the other five violations.

The Commander should also be made aware of the presence of hospitals and/or schools in his AOR, so that he may plan around these appropriately. Finally awareness of CAAC and its incorporation in planning in different phases of the conflict is important to establish legitimacy for the force. Both with the host populace, as well as with the population back home.

> *"The protection of children from armed conflict is an important aspect of a comprehensive strategy towards resolving conflict and building a durable peace. It is thus a legal obligation and a matter of peace and security."*
>
> Civil-Military Cooperation
> Centre of Excellence

Responsibilities in CMI

Different branches outside of J9 have a responsibility regarding CAAC. J2 provides analysis on presence of CAAC in the AOO. J3 and J5 have to include CAAC considerations into plans and operations.

J-MED has to make sure there is proper psychological support for soldiers dealing with CAAC. The LEGAD has to provide advice on CAAC within International Law and Humanitarian Law, and the obligations this entails. Finally J7 has to provide pre-deployment training on how to deal with CAAC on a mission.

Legal Implications

CAAC is extensively covered in international law. Recruitment is prohibited under IHL, and offenders can be prosecuted by the ICC. Violence against civilians, including children, is prohibited under the Geneva Conventions. This is universally applicable and is binding for government and non-government military actors.

When confronted with child soldiers, military personal may legally defend themselves, but have to take into account the principle of proportionality. The Commander needs to be aware of these prohibitions.

Because armed forces committing the six grave violations can be prosecuted, it is imperative that these violations, when observed, are reported. These reports can later be used as evidence.

Cross-Cutting Topics (CCT)

CAAC is interlinked with several of the other CCTs. Firstly, it fits under the broader issue of Gender. Gender deals with women, men, boys, and girls, and thus with CAAC. Incorporating a gender perspective is therefore imperative when dealing with CAAC.

Secondly, CAAC also fits under Protection of Civilians. POC is the broader issue dealing with all civilians, and protecting children is a part of this responsibility.

And thirdly, Rule of Law is important, as the legal protection provided to children requires a working RoL. The threat of prosecution can also inhibit the harming of children in conflict.

Assessment Implications

CAAC should be included in the CIMIC estimate, and on assessments on all levels. The assessments should include the role and situation of children in the civil society as well as the various organizations working on the topic. Special attention should be given to the presence of Children Associated with Armed Forces or Armed Groups (CAAFAG) child soldiers in the AOR. In addition the presence of hospitals and schools in the AOR has to be included. Because a large part of the responsibility to deal with CAAC lies with IOs and NGOs, it is wise to share these assessments with civil partners. In reverse IOs and NGOs will be able to provide in-depth information on CAAC in the mission area, and how best to protect them.

Leading Organizations

Within the UN Cluster approach, CAAC falls firstly under the Protection Cluster, led by the UNHCR with NGOs like Save the Children, International Rescue Committee, War Child as well as other UN agencies like UNICEF also represented. The Education Cluster is also important, co-led by UNICEF and Save the Children. Outside of the Clusters, UNOCHA, the Office of the Special Representative of the Secretary-General for Children and Armed Conflict and other relevant UN/EU or AU can provide information and assistance.

In addition the EEAS of the EU, and the AU deal with CAAC. Within NATO there is not one entity in charge of dealing with CAAC.

Point of Contact during Mission:

IOs and NGOs will have the best view on the presence of CAAC in the area. Therefore policy officials of the different leading organisations and project leaders of important NGOs in the AOR, like World Vision and Watchlist on Children and Armed Conflict should always be contacted. The IOs and NGOs can also explain in what way they are engaged with the local population. If they are not in contact with local administrators responsible for schools and hospitals, contact should be established by the CIMIC unit.

Sources of Additional Information:

- https://www.savethechildren.net/
- http://www.unicef.org/
- https://childrenandarmedconflict.un.org/

References:

- United Nations, Office of the Special Representative of the Secretary General for Children and Armed Conflict https://childrenandarmedconflict.un.org/effects-of-conflict/six-grave-violations/
- Office of the Special Representative of the Secretary-General for Children and Armed Conflict (2013), The Six Grave Violations Against Children During Armed Conflict: The Legal Foundation.
- Civil-Military Cooperation Centre of Excellence (2014), CIMIC Messenger 6(3)
- Center for Emerging Threats and Opportunities (2002), Child Soldiers: Implications for US Forces

The “Do’s” and “Don’ts”:

Do’s

- Observe and report violations of international law.
- Refer children whose rights are being violated to the appropriate IOs and NGOs in the AOR.
- Understand and respect the mandates of present humanitarian organizations.
- Support IOs and NGOs in the AOR who have experience with working with CAAC in the mission area.
- Appoint CAAC focal points within branches and/or units.

Don’ts

- Do not ignore the proportionality principle when forced to engage child soldiers.
- Do not cause damage to schools and hospitals.
- Do not leave the Commander and the force unprepared for possible encounters with children.
- Do not allow the use of children as support for military forces, i.e. as cooks or porters, this is also identified as using child soldiers under IHL.

CIMIC Tasks:

- Liaising with IOs and NGOs to gather information on CAAC and closely cooperate with these same actors in dealing with CAAC.
- Enabling the sharing of information concerning CAAC, for example CIMIC assessments, with IOs and NGOs in the AOR.
- Teaching military personal how to properly engage with children in the mission area according to legal obligations.
- Providing information on the civil situation, which includes considering the situation of children as bystanders in the conflict and/ or as active participants in the conflict.
- Identifying civil key indicators and sensitive factors regarding

CAAC which may critically impact the conduct of operations as well as the impact of military activities on the civil environment.

- Help with the identification of child soldier recruitment zones.
- Advice on offering protection for demobilized child soldiers against revenge seeking locals and rebel forces seeking to recruit.

Good Governance & CIMIC

A CCOE Fact Sheet

Introduction:

Governance means: “the process of decision-making and the process by which decisions are implemented (or not implemented).” (UNESCAP 10-2009)

There is no NATO agreed definition on ‘Good Governance’. Within the international community each organisation has their own view on Good Governance. There are several characteristics stated by the UN that are widely accepted as desirable.

Good Governance should be “participatory, consensus oriented, accountable, transparent, responsive, effective and efficient, equitable and inclusive and [it] follows the rule of law. It assures that corruption is minimized, the views of minorities are taken into account and that the voices of the most vulnerable in society are heard in decision-making. It is also responsive to the present and future needs of society.” (UNESCAP 10-2009)

> *“Good Governance is of high interest and value for military operations, because it is a key component to achieve sustained success of a mission. As a prerequisite for political ownership and therefore as a part of the desired end state, the high mission relevance of Good Governance becomes visible.”*
>
> *Civil-Military Cooperation*
> *Centre of Excellence*

Mission Implications:

Many crises and conflicts has their root cause in bad governance in the country. Therefor the term Good Governance is frequently used to describe a range of solutions which could be used to improve/ solve this root cause. The responsibility for the establishment of Good Governance lies with the Host Nation (HN) often with extensive support from International Organisations (IO), Non-Governmental Organisations (NGO) or Governmental Organisations (GO). The impact that Bad Governance has, can also affect and hamper the success of a military mission.

A first step towards Good Governance is the creation of a safe and secure environment (SASE) in which the HN together with other actors (IO, NGO, GO) can do their work. This SASE is the responsibility of the HN, however in most cases a military mission can support or even take over temporarily that responsibility if needed. That responsibility needs always to be shared with the HN. The goal of this shared responsibility is the promotion of trust and local ownership. This can be promoted by professionalising the security services, and increasing contact between the local population and the government.

A lack of Good Governance in a mission area can make it difficult to cooperate with the local authorities and can spark violence amongst the population and towards the military mission.

Legal Implications:

A Government is obligated to protect and provide basic services for their citizens. In many crises/conflict areas the government is not able or willing to fulfil these obligations. Good Governance facilitates these obligations, therefor Rule of Law and Building integrity should be fully integrated in Good Governance.

Many of the standards of Good Governance are backed by international law. E.g. Human rights are formalized in the Universal Declaration of Human Rights, international treaties, and in Customary International Law and International Humanitarian Law.

Whereas on a National level Good Governance might follow the international standards, on the regional and local level this might not be the case.

Assessment Implications:

What constitutes as Good Governance, can be difficult to assess. The style of governance is strongly based on culture of a nation. By applying a cultural competence model (coping with culture, CCOE) will significant increase insights into the workings of the style of government.

CIMIC personnel plays a vital role in to assessing and evaluating the criteria of Good Governance. By using PMESII (Political, Military, Economic, Social, Information and infrastructure) and ASCOPE (Area, Structures, Capabilities, Organisations, People and events)as a means to asses in particular or situational cases. With the goal to incorporated it into military planning and assessment.

This assessment helps to create understanding what consequences military actions can have on the HN governmental structures. This can assessment can be achieved to follow four steps.
These steps are:

1. **Define** governance-related objectives based on the mandate (what is expected from the military mission in relation to support the HN government).

2. **Identify** positive, negative, and neutral factors which influence the military objectives (which actors will contribute, hamper the support to good governance).

3. **Determine** tools to strengthen positive, mitigate negative, and turn neutral factors (what is needed as actions to improve the government).

4. **Assess** achieved effect and re-evaluate if necessary (which means are in or should be in place that can track and asses the progress).

Leading Organisations:

The United Nations promotes Good Governance through several avenues, the IMF provides lending and technical assistance, and UNDEF supports projects that strengthen the voice of civil society, promote human rights, and encourage the participation of all groups in democratic processes.

The EU, the AU and the World Bank also run several programmes supporting Good Governance. NATO on an operational/tactical level does not have a leading branch/body responsible for Good Governance, currently within NATO only the CCT Building integrity and Rule of Law are indirectly connected to it.

Responsibilities in CMI:

Different branches outside of J9 have an impact on the success of Good Governance. The J2 provides in collaboration with J9 an analysis on the governance situation. J3 and J5 have to include good governance considerations into plans and operations. In particular they have to incorporate the route towards a situation where responsibilities can be transferred to civil partners. J4 has to be aware how their procurement and logistical activities impacts the local power structure. The advisors need to give input from their specific area on Good Governance.

Cross Cutting Topics:

Good Governance could be seen as the framework necessary for the proper incorporation of other Cross Cutting Topics. Proper integration of a **Gender** perspective in society requires a participatory, inclusive government. The establishment of working **Rule of Law** is one of the most important aspects of good governance.

Cultural Property Protection, Protection of Civilians, and Building Integrity require Good Governance, with a monopoly on violence and an established Rule of Law.

Point of Contact during the Mission:

A constant communication between the military Force including de senior civilian component and the local and regional authorities is key into the understanding of Good Governance. Leading organisations on Good Governance are UNDP, Transparency International, The International Foundation for Electoral Systems, the Carter Centre, and Freedom House, should be Liaised with in order to share information and work towards common goals.

Sources of Additional Information:

- Information on performing a good governance assessment can be found in the CCOE publication Good Governance Makes Sense: https://www.cimic-coe.org/products/conceptual-design/downloads/ccoe-publications/makes-sense-series/
- The Centre for Integrity in the Defence Sector has published multiple guides on Good Governance: http://cids.no/goodgovernance
- The Geneva Centre for Democratic Control of the Armed Forces has Good Governance as one of its main focus points: http://www.dcaf.ch/goodgovernance
- The World Bank: The World Bank Governance Index / World Bank's Governance Global Practice

References:

- United Nations Economic and Social Commission for Asia and the Pacific (2009), what is Good Governance?
- Supreme Headquarter Allied Powers Europe (2012), ACO MANUAL 86-1-1
- Centre for integrity in the Defence sector

Do’s and Don’ts:

Do’s

- Be aware of the existence of different ideas about ‘good’ governance.
- Realize that different priorities, exist which can differ on local in comparison with national levels.
- Promote local ownership, capacity and leadership.
- Use assessments made on the operational/higher level as a starting point (startegic and operational level).
- Identify key personnel within the mission (all levels) that are responsible for governance related issues
- Identify key players either national/local and international (IO, NGO, GO) and establish contact.
- Track money flows and identify the power structures that are behind it. These are key elements which provides a better insight into the governance structures.
- Promote/explain the military involvement with the Host Nation authorities.
- Take into account cultural shaping factors and phenomena, when assessing governance in the mission area. A different religion or history can mean a different interpretation of good governance.

Don’ts

- Do not try to achieve ‘good’ governance alone. It requires a comprehensive approach and to provide a safe and secure environment.
- Do not assume control of decision-making in the mission area. Be a partner, not a patron.
- Do not deal with known corrupt officials.
- Do not give premature advice on how to solve governmental issues, we are not experts.
- Do not judge governmental styles.
- Do not presume good governance is achievable overnight. It is a long-term, incremental process, requiring multiple actors.

CIMIC Tasks:

- Collecting information on Good Governance in the area to enhance situational awareness.
- Identifying which essential requirements in a particular situation or area are needed to support or develop trust among the different actors involved in the process of governing.
- Analysing how government support/capacity building programs are being implemented by IOs, GOs and NGOs and which could be supported within our means and capabilities.
- Establishing and maintaining routine contacts and ensuring effective and constant communication with all non-military actors working on governance.
- Assisting with and monitor of governance projects, which can influence the military mission, such as elections, establishing new governmental structures or telecommunication.
- Establishing and promoting transparent and accountable interaction with communities, IOT make sure that a co-operative image of the military force together with our counterparts, either the international community as well as the HN authorities is promoted.
- Supporting the Military mission by explaining our presence and intent of the mission to our contacts within the international community and the local environment.

Women, Peace and Security

A CCOE Fact Sheet

Introduction:

UN Security Council Resolution (UNSCR) 1325 from October 2000 was the first UN Security Council resolution to acknowledge women's and girls' involvement in conflict and their central role in the prevention and resolution of conflicts, as well as in peace consolidation. In 18 paragraphs, the Council appealed for the greater participation of women in decision-making; their further engagement with peacekeeping, field operations, mission consultation and peace negotiations; increased funding and other support for UN bodies' gender work; enhanced state commitments to women's and girls' human rights and their protection under international law; the introduction of special measures against sexual violence in armed conflict; and the consideration of women's and girls' needs in humanitarian, refugee, disarmament and post-conflict settings[1].

NATO and the Women, Peace and Security mandate are fundamentally connected through the common values of individual liberty, human rights, and obligations under the Charter of the United Nations. In line with the UNSCR 1325, NATO aims to address gender inequality and integrate WPS through the Alliance's three core tasks of collective defence, crisis management and cooperative security. NATO and its partners recognize that the impact of conflict and post-conflict situations is disproportionate on women and girls, and contribute to the full implementation of the WPS agenda, supporting its advance through the guiding principles of integration, inclusiveness, and integrity[2]. Although NATO's gender definition encompasses men, women, girls and boys, the WPS agenda is directly related to gender, but with a focus on women and girls' rights and protection.

[1] KIRBY, P. and SHEPHERD, L. (2016). Reintroducing women, peace and security. International Affairs, 92(2), pp.249-254.

[2] Special Representative to the Secretary General on Sexual Violence in Conflict Margot Wallström (2010). Keynote Speech At The Women And War UNSCR 1325 Tenth Anniversary Conference.

Legal Implications

The basic legal framework begins with the **Universal Declaration of Human Rights (1948)**, stating that all humans should be treated equally regardless of gender. This is strengthened by the **Convention on the Elimination of All Forms of Discrimination against Women - CEDAW (1979)** and the **Beijing Declaration and Platform** for Action adopted at **The Fourth World Conference on Women (1995)**.

UNSCR 1325 (2000) and related Resolutions 1820 (2008), 1888 (2009), 1889 (2009), 1960 (2010), 2106 (2013), 2122 (2013), 2242 (2015), 2272 (2016) provide guidance and enhance efforts to promote and protect the rights of women in conflict and post-conflict situations.
NATO has pledged to implement the UNSCR 1325 through the adoption of their **Bi-SC Directive 40-1 Integrating UNSCR 1325 and Gender Perspectives into the Command Structure**, including measures for protection during armed conflict.

Mission Implications

Within the framework of the comprehensive approach, the protection of the entire society must be addressed, highlighting the differing security concerns, risks and experiences that women and girls have. If the protection of civilians against gender-based violence is not taken into account, it can have an impact on the sustainability of mission results.

The important roles of women in the prevention and resolution of conflicts and in peace-building, and their equal participation and full involvement in all efforts for the maintenance and promotion of peace and security must be seen as a relevant part of the mission. A mixed gender force enhances the sharing of information and is instrumental in garnering trust and credibility.

At all phases of the mission the commander should enforce the application of NATO standards of behavior and respect to international humanitarian law and human rights law on protection of women and girls' rights. The commander should include a gender perspective into planning and execution of operations to be able to implement the WPS agenda.

Assessment Implications

The different perspectives from men and women in the society have to be included for a comprehensive understanding of the civil environment. Thus a gender perspective has to be included in the civil estimate, and in other assessments and reports.

Specifically the presence of gender based violence in the AOR and possible countermeasures need to be assessed and conveyed to the commander.

Integrating gender perspective is done by adapting action following a gender analysis. Gender analysis requires the systematic gathering and examination of information on gender differences and on social relations between men and women in order to identify and understand inequities based on gender.

Responsibilities

- J1 – Responsible for the gender balanced recruitment of work force to engage with the civilian population.
- J3 – Integration of gender awareness in the execution of operations.
- J5 – Integration of gender awareness in the planning process of operations.
- J7 – Collective training and exercise on gender awareness and gender mainstreaming, including in pre-deployment training.
- J9 – Ensure the relevance of the WPS cross-cutting topic in all force activities. Advising the commander on WPS.
- LEGAD and GENAD – Assess and advice on the legal and mission implications that relate to WPS.

UN Women - global advocate and responsible for supporting mission actors with technical expertise on WPS.

United Nations Department of Peacekeeping Operations (DPKO) - mandated by the Security Council to implement the Security Council Resolutions on WPS across all peacekeeping functions.

NATO - the Special Representative for Women, Peace and Security serves as the high-level focal point for NATO's contributions to the WPS agenda.
EU - the European Institute for Gender Equality (EIGE) works on promoting gender equality.

OECD – the Development Assistance Committee (DAC) provides aid to gender equality in fragile states and economies.

U.S. Institute of Peace (USIP) - provides training, analysis, and other resources to people, organizations, and governments working for gender equality and protection for women and girls.

Working Group on Women and Armed Conflict - monitors policy and practice and builds coalitions between civil society and high-level decision makers to advance the WPS agenda.

Nordic Centre for Gender in Military Operations (NCGM) - provides advice on policy development, holding T&E courses, and participating in seminars and workshops.

Related Topics:

The Women, Peace and Security agenda is strongly linked to several other important topics. WPS is related to **Protection of Civilians** and the Responsibility to Protect. The WPS pillars of protection and prevention call for the protection of women and girls from sexual and gender-based violence.
The **Children and Armed Conflict** topic is connected to WPS, because of the need of a gender perspective related to the protection of children in conflict situations and the rehabilitation and social reintegration process, and the prevention of gender-based violence.
Good Governance requires (gender) equality. The UNSCR 1325 on WPS calls for measures to ensure the protection and respect for the rights of women and girls, particularly as they can be related to the host nation's

constitution, the electoral system, the police and the judiciary. WPS is supported by a working **Rule of Law**. The prevention pillar of WPS demands the prosecution of those responsible for violations of international law, the strengthening of women's rights under national laws. **Disarmament, demobilization, and reintegration (DDR)** and security sector reform (SSR) are relevant to the WPS agenda as one of its pillars is about relief and recovery, including in the mandate the special needs of women and girls involved in armed conflicts during repatriation and resettlement and for rehabilitation, reintegration and post-conflict reconstruction.

Points of Contact during the Mission:

The responsibility to ensure the implementation of the UNSCR 1325 on WPS lies within the local authorities that are supported by GOs, NGOs and IOs.

- Local government
- UN Women: http://www.unwomen.org
- DPKO: https://peacekeeping.un.org/en/promoting-wom en-peace-and-security
- USIP: https://www.usip.org
- NGOs
- NATO: IMS Office of the Gender Advisor - dgims.genad@hq.nato.int
- NCGM: http://www.forsvarsmakten.se/en/swedint

Sources of Additional Information:

- On NATO Women, Peace and Security, http://www.nato.int/cps/en/natohq/topics_91091.htm
- On WPS policy implementation www.peacewomen.org
- On gender in humanitarian operations, https://www.humanitarian response.info/en/topics/gender
- The NCGM website provides information on gender and on available gender courses, http://www.forsvarsmakten.se/en/swed int/nordic-centre-for-gender-in-military-operations/

References:

- UN Security Council, Security Council resolution 1325 (2000) [on women and peace and security], 31 October 2000, S/RES/1325 (UNSC, 2000)
- CCOE/S. Groothedde, Gender Makes Sense: A Way To Improve Your Mission, Second Edition (CCOE, 2013).
- NATO, BI-SC Directive 40-1 (NATO, 2012).
- NATO/EAPC, Women, Peace and Security: Policy and Action Plan (NATO, 2018).
- NATO, AJP-3.19 Allied Joint Doctrine for Civil-Military Cooperation (NATO, 2018).
- UN Entity for Gender Equality and the Empowerment of Women, Preventing Conflict Transforming Justice Securing the Peace - A Global Study on the Implementation of United Nations Security Council resolution 1325, 12 October 2015 (UNWOMEN, 2015)

The "Dos" and "Don'ts":

Dos

- Harmonize WPS activities with NGOs and IO, to avoid duplication of efforts.
- Adhere to NATO standards of behavior and the UN zero tolerance policy on sexual exploitation and abuse.
- Report violations to the chain of command.
- Reach out to gender specialists when necessary.
- Include gender analysis on the civil assessment.
- Support local women's peace initiatives and facilitate their active inclusion in the conflict resolution and peace building processes.
- Be aware of the "feel good trap" (doing things because they give you a good feeling but are not necessarily sustainable or effective) related to implementing WPS.

Don’ts

- Don’t stereotype gender roles.
- Don’t set up WPS related activities outside the boundaries of the mission.
- Don’t ignore local customs and traditions relating to gender.
- Don’t create barriers between military and non-military actors working on the implementation of the WPS agenda.
- Don’t close your eyes to a situation of discrimination based on gender.
- Don’t assume that working on gender and/or WPS is only for or about women.
- Don’t minimize or ignore the contributions of women and girls in conflict and post-conflict situations.
- Don’t consider WPS a standalone topic. It is a cross-cutting topic and affects all lines of operations.

CIMIC Tasks:

- Establish and maintain liaison with local authorities, local population, NGOs and IOs dealing with gender and the implementation of the WPS agenda.
- Include WPS and gender in education and training.
- Perform gender analysis: the systematic gathering and examination of information on gender differences and social relations to identify and understand inequities.
- Include gender issues in the standard reporting procedures, with special attention being paid to sexual violence and other transgressions. Reports can be used as evidence in the court of law.
- Inform fellow soldiers on local laws, customs, culture and traditions regarding gender.
- Promote force acceptance by including a gender perspective.
- Provide of information on the civil situation, taking into account the gender dimensions of the civil situation.
- Enable and provide support to the implementation of WPS by means of capacity building and capacity sharing on gender.