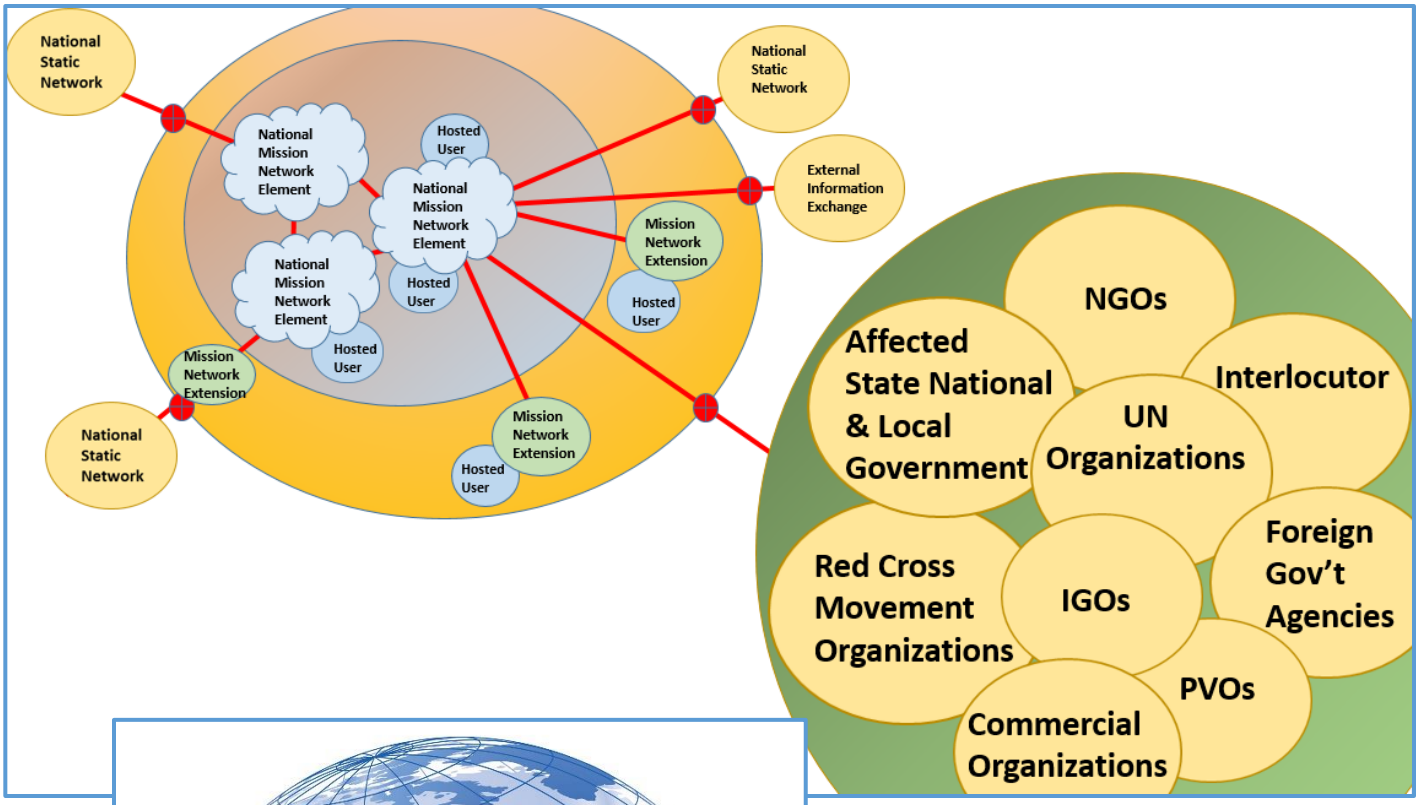
Operational Concept

for

CIVILIAN-MILITARY INFORMATION SHARING IN A FEDERATED MISSION NETWORKING ENVIRONMENT



MCDC

Multinational Capability Development Campaign

MCDC 20015-2016: FMCM Operational Concept

Questions or comments can be referred to: MCDC_SECRETARIAT@APAN.ORG

PARTICIPANTS & ROLES:

Project Lead(s): USA, NATO ACT

Contributing Nations & Organizations: NATO ACT, European Defense Agency, Canada, Netherlands, Sweden, Switzerland, USA

Observers: United Kingdom, UN OCHA

Table of Contents

Title/paragraph **Page Number**

Executive Summary……1

Preface……4

Section 1: Capability Need ……5

1.1 Information Sharing Construct…….....6

1.2 Current Capability and Gaps……...……...……...10

1.3 Capability Development of CMIS……...…….....11

Section 2: Operations and Support Descriptions……..……15

2.1 Missions……...……15

2.2 Stakeholders……16

2.3 Assumptions and Constraints……...……...18

2.4 Capability Description…….……...…..18

2.5 CMIS Employment in FMN…….……18

2.6 Potential Impact of CMIS……...……..19

Section 3: Use Cases……20

3.1 Operational Scenarios……...……..20

3.2 CMIS Operations Use Cases…….……..22

Section 4: Functional Capabilities……25

Section 5: Appendices……26

5.1 Glossary of Terms and Acronym Listing……..26

5.2 References……..32

EXECUTIVE SUMMARY

Effective information sharing between military and civilian actors operating or collocated in the same mission area is essential for the strategic success of the mission. There are challenges to every mission and inaccurate or insufficient information sharing between military and civilian actors will only intensify those challenges.

This Operational Concept, entitled Civilian- Military Information Sharing in a Federated Mission Networking Environment (CMIS) identifies a methodology and framework in which information can be shared between civilian and military actors. Military actors refers to any organization planning or conducting operations where information must be shared with civilians who are not members of the secure network environment. The Operational Concept assumes that some or all military actors are sharing information within a Federated Mission Networking (FMN) environment. The intent is to inform military actors how better to share information with civilians.

FMN provides instructions for rapidly forming a federation of multinational military networks, leveraging agreed standards and protocols to create a common information environment. Extending beyond the FMN boundary, information sharing becomes more challenging. What can be shared, with whom, where, when and how is determined by each military or civilian actor in accordance with policies, individual needs, constraints and decision-making processes.

This concept is not intended to change how governments, militaries, international organizations or humanitarian communities conduct their business nor does it mandate the sharing of information or require organizations to modify their inter-relationships. Rather, it describes FMN capabilities that will be required to share information between FMN participants and non-FMN entities, including Non-Governmental Organizations (NGOs), International Organizations (IOs) and private sector organizations.

The CMIS Operational Concept is intended for use by military forces when planning and executing information sharing with civilians. It is focused on mission environments in which FMN is deployed and provides a framework for information sharing during peacekeeping support and humanitarian operations. **The goal of the Operational Concept is to increase mission success through enhanced CIV-MIL information sharing.**

Inconsistent military information sharing practices and standards inhibit the establishment of a CMIS environment. The intent of this concept is to support effective information flow

between civilian and military participants across the spectrum of military operations and different types of situations on-the-ground. Operations may range from rapid onset humanitarian assistance and disaster response in a benign cooperative environment to complex emergencies and armed conflict in which civilian activities and military operations at best can merely coexist.

Commanders must ensure CMIS frameworks are in place to support planning and execution of effective information sharing and that CMIS, including technical means and competencies, is part of normal operating capabilities. The FMN environment must be configurable to allow information sharing between classified networks and the publicly accessible internet. This may require the use of multi-level security and cross-domain gateways to control the flow of information.

CMIS has the following objectives:

- To use common standards that improve information sharing between civilian and military actors;
- To improve mutual understanding of military and civilian information management and planning processes; and
- To reduce the planning time required to establish information sharing between military and civilian actors.

The Operational Concept describes the environment and requirements to conduct CMIS in a range of operating environments. The CMIS Guidebook, based on the operating environment, recommends information sharing venues and best practices to effectively establish and facilitate information sharing outside the military network environment. The effort seeks to address the following documented CMIS deficiencies:

- Lack of mutual trust in information protection and sharing.
- Military forces not understanding humanitarian community organizations, operations, policies, and purposes.
- Information sharing processes are neither standardized nor supported by best practices.
- Military use of classified systems for unclassified operations.
- Insufficient specific military capability or authority as an information release specialist (i.e. Foreign Disclosure Officer).
- Military functioning as independent responders, not in coordination with the affected state and humanitarian communities.
- Military responders do not collaborate and fail to achieve unity of effort.

- Lack of shared situational awareness and an inability to share a common operating picture and unclassified imagery or video.
- Improper security classification designations by military entities intending to share information (i.e. For Official Use Only - FOUO) restricts sharing information outside government channels that should be marked "For Public Release".
- Lack of CIV-MIL information sharing planning to include:
    - What information is needed
    - Who has release authorization
    - Where/who needs the information
    - What form is the information needed to be usable

PREFACE

This Operational Concept describes capabilities available to create effective CIV-MIL information sharing. Central to this concept is the recognition that **a balance of cooperation and independence is paramount to the success of the information sharing relationship**. The amount and types of information that the civilian and military actors will be willing and able to share with each other is situationally dependent and based on trust. The level of trust available to civilian and military actors operating in the same mission area will be pre-existing, based on institutional norms and previous experience. Trust also will evolve, based on on-the-ground experience.

Trust must be created and maintained between CIV-MIL participants in the mission space. In the CIV-MIL information sharing environment, procedures are insufficient to establishing and maintaining trust. Trust must be established at the organizational and personal levels. Humanitarian organizations especially will consider any risk to their ability to access an affected population, including physical risk to the affected population and field staff. Civilians in general tend to be focused more on personal rather than just organizational factors. Trust considerations may include operational risks outside the affected state where humanitarian organizations are operating.

The requirement for military actors to interact and coordinate with civilians exists in all modern operations and coordination can only be achieved through effective information sharing. Regardless of the nature of the engagement, military planners and deploying staffs need to understand the relationship they have with collocated civilian organizations and the level of coordination needed to successfully complete the mission.

When a mission is established, coordination between militaries occurs on a mission network. The mission networking environment considered in this operational concept is the Federated Mission Networking (FMN) environment. FMN consists of a federation of individual mission networks that exchange information based on standards and processes agreed between the contributing militaries. More details of the FMN concept are provided in references A-F.

Note: For simplicity, the Operational Concept will use the singular term FMN to represent a unified, rapid effort to establish a mutually supported information-sharing environment between mission partners. MPE is the US implementation of the FMN development effort and is compatible with FMN structures.

SECTION 1: CAPABILITY NEED

The Federated Mission Networking (FMN) is a federation of mission networks provided by contributing militaries. FMN provides a classified environment and the means for sharing information within the federation but not currently with external actors. This document describes the concept of extending information sharing to non-FMN actors operating outside of the protected environment in an unclassified public space. This concept is depicted in Figure 1, which shows the FMN environment in the upper left connected to the unclassified civilian environment in the lower right hand corner of the figure. Within the FMN environment, information is sharable and accessible by all network participants. For entities existing outside the FMN environment, the FMN capability must include external gateways that control information flows between the secure information environment and the public internet where the majority of civilian actors will be.

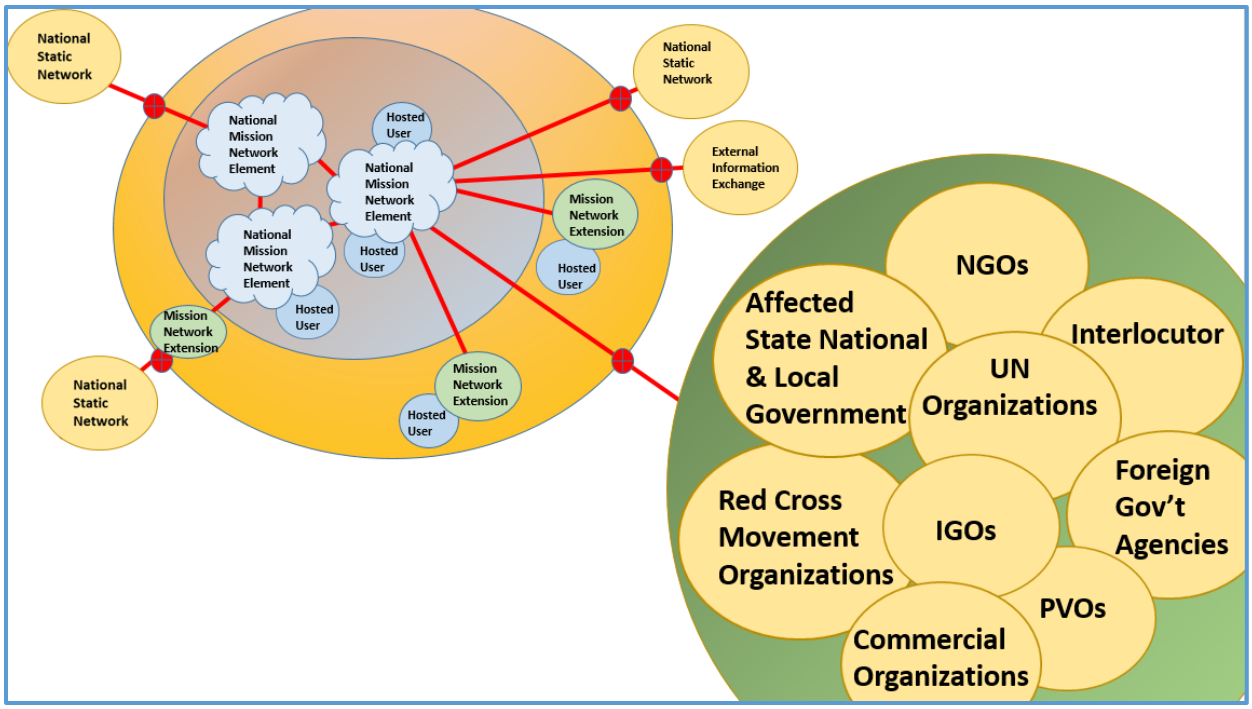


Figure 1

1.1. Information Sharing Construct

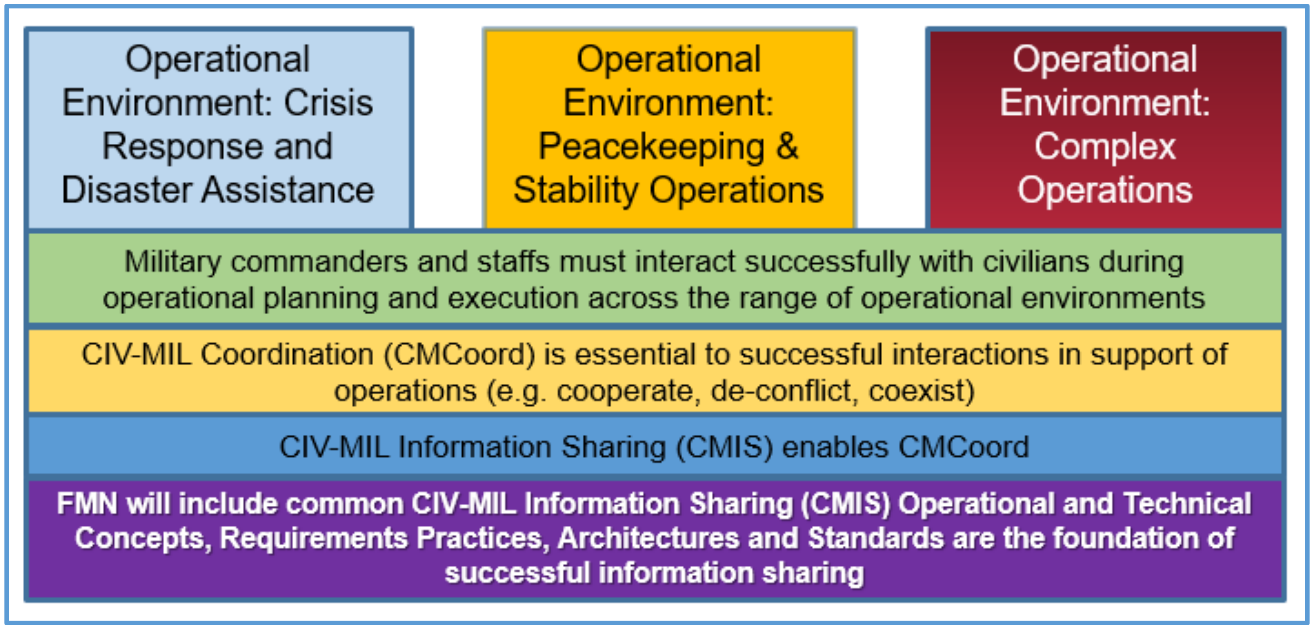


Figure 2

Figure 2 depicts the imperatives for interaction and coordination which create the requirement for CMIS. It recognizes that the controllable variable during interaction is the behavior and capability of the military in CMIS. The military will encounter a variety of civilian actors in the theater and area of operations. These can include affected state government and agencies, foreign government agencies, international and local non-government agencies, humanitarian organizations, and private entities. The competence of the military in CMIS will affect the civilian's willingness to share information.

Humanitarians serve a critical role but have a different focus: save lives, alleviate suffering; whilst maintaining the dignity of those in need. Their efforts are applied uniformly in any environment where their support is needed. This is regardless as to whether the humanitarian crisis results from natural disaster or is man-made.

1.1.1 Federated Mission Networking

FMN hosts information exchange services used by the military participants. These services include Voice-Over-Internet-Protocol (VOIP), email with attachments, video teleconference, chat, web browsing, and directory and other services that support joint and combined operations. The FMN environment is typically classified and will require an unclassified environment and/or gateway to exchange services with external non-FMN actors.

1.1.2 Essential CMIS Interactions

Even before executing a mission, military planning and pre-deployment phases will need to identify essential CIV-MIL information sharing interactions at the strategic, operational and tactical levels. Planning for CMIS ideally will involve significant input from Civil-Military Coordination experts and Civil Affairs specialists. These specialists will help develop CMIS tasking orders, establish contacts with key civilian organizations in the area of operation and provide access to tools, including web portals and mobile applications that support information sharing amongst civilian entities.

1.1.3 CIV-MIL Coordination in Support of Operations

The required level of sharing between military and civilian actors will depend on the nature of the mission. In complex environments involving combat operations, it is not uncommon for CMIS to be restrictive. In a stable environments CMIS can be open and direct. Effective CMIS requires military actors to take a flexible approach and be adaptable to different levels of willingness-to-share by civilian actors.

1.1.4 CMIS Operational Planning and Execution

Effective planning and execution of CMIS requires military actors to have awareness of the humanitarian principles of humanity, neutrality, impartiality and independence and to understand the significant importance humanitarian actors place on trust. Actions or inaction by military actors will either support or degrade this trust. Once degraded, trust can be difficult to restore. Planners must consider the driving factors in CIV-MIL interaction; trust, shared goals, and mutual acknowledgement that CIMIS is necessary. The personality of key actors will have a significant impact on CIV-MIL dynamics.

1.1.5 Operational Environments

This operational concept describes three operational environments:

- Stable environments characterized by humanitarian crisis response and disaster assistance. In this case military and civilian actors can cooperate to achieve a common goal;
- Less stable environments characterized by peacekeeping/stability operations. In this case military and civilian actors need to de-conflict their activities to maintain safety, security, efficiency and effectiveness; and
- Complex environments characterized by combat operations. In this case military and civilian actors will coexist with minimal or no contact.

1.1.5.1 Stable Environments – Crisis Response and Disaster Assistance

During crisis response and disaster assistance, the military actors will establish an FMN environment to share information and coordinate their support operations through the Multi-

National Military Coordination Center (MNMCC). The MNMCC serves as the interface between the affected state and the responding military forces and is responsible for coordinating actions among all multinational military forces.

In UN-coordinated operations, the MNMCC will work closely with the Humanitarian Military Operations Coordination Center (HuMOCC) to parse, validate, and assign civilian Requests for Assistance (RFAs) to the supporting military forces. The HuMOCC is a means by which requests for military assistance can be submitted. In addition to the UN, the National Society of the Red Cross of the affected state, working closely with the International Federation of the Red Cross, may act as coordinating authority for assisting state Red Cross and Red Crescent elements from other nations. National Red Cross and Red Crescent societies often have a chartered relationship with their government and military.

CMIS provides the ability for military actors within the FMN environment to share information with civilian humanitarian actors via multiple paths; either in conjunction with the HuMOCC, through other coordinating organizations and/or via interlocutors.

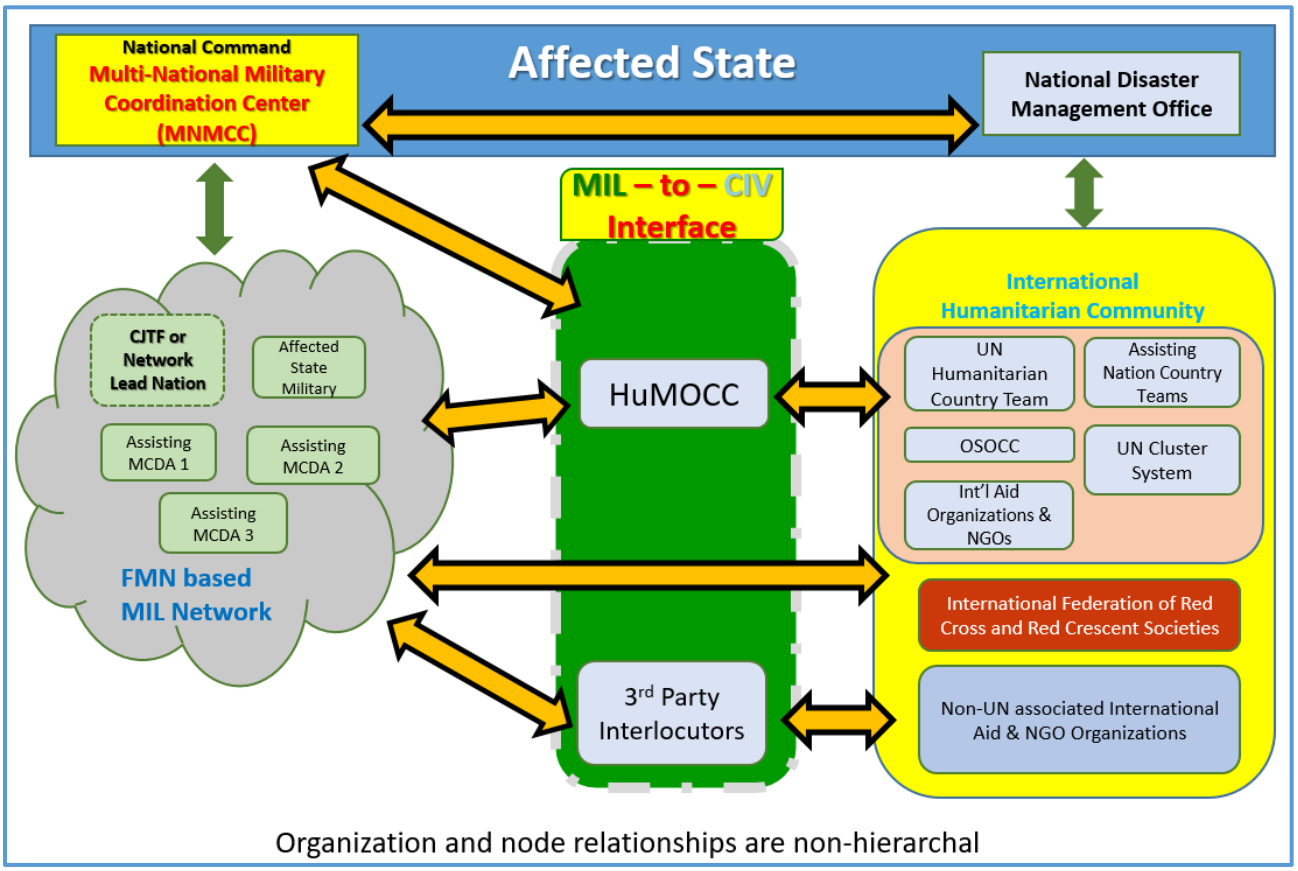


Figure 3

Non-UN based organizations may go directly to the military's operation center, or the government's civilian development and humanitarian agency. In the case of the US, this would be the United States Office of Foreign Assistance (OFDA) and the Agency for International Development (USAID).

Some major aid agencies and assisting nations may not utilize the UN HuMOCC, but rather conduct their national response through affected state offices, national military and/or host nations. For sovereignty reasons, affected states may favor direct contact or direct liaison with the humanitarian community and the MNMCC. Humanitarian agencies in country pre-crisis will have a network of contacts with affected state agencies as well as with opposition groups as a primary means of access and security for their operations. Assisting state military organizations must respect national lines of authority and the affected state's sovereignty and not disrupt this structure

1.1.5.2. Peacekeeping/Stability Operations

Peacekeeping and Stability Operations missions involve coordination with many international and national actors operating in proximity during a post-conflict period. Difficulties establishing trust between civilian and military actors during this time often preclude the establishment of a common information sharing structure. In these operations effective CMIS is difficult but can be achieved through regular meetings, information sharing processes and establishing dialog with key non-military entities at national and local levels. Key non-military entities include:

- United Nations field leadership and operations centers
- Foreign non-military governmental agencies
- Independent humanitarian actors (non-UN based), especially those associated with the International Committee of the Red Cross (ICRC)
- Affected state government at the national and local level
- Contracted security forces

Organizations and foreign government entities responding to a peacekeeping and stability mission normally pursue independent objectives which may not align with the responding military's operations. Some may use different timelines or methods, or not engage at all in cooperation and information sharing. Nevertheless, an information sharing strategy should be created regardless of level of engagement and coincidence of objectives.

Some humanitarian actors, such as the ICRC, have an institutional imperative to maintain a visible impartiality from political (UN) and military structures to ensure safety and independence of their actions and personnel. In peacekeeping and stability operations military actors must be aware of and respect this "humanitarian space." Peacekeeping missions must recognize the distinction between politically motivated actions to end conflict and support national development and apolitical humanitarian assistance based on impartial needs assessments and responses.

1.1.5.3. Complex Operations

Complex operations include combat or high threat environments. HA/DR events can be complex due to threats such as industrial chemical, pandemic or nuclear incidents. During complex operations it is important for military planners to know the locations of humanitarian actors to avoid targeting them and to support humanitarian protection operations. It is equally important to maintain humanitarian independence by not unwittingly mixing humanitarian and combat forces.

The military should share threat information about mines, roadside bombs, other explosive devices and armed groups that may not respect humanitarian neutrality. Military actors must be mindful that the affected population may be hostile to military forces, which could lead to direct threats to humanitarians seen to be collaborating with the military. This does not negate the need to share information but emphasizes the importance of careful CMIS planning. In complex operations civilian actors can request assistance from and communicate with the military through an interlocutor who functions as an intermediary. An interlocutor may be an organization, individual or government representative.

1.2 Current Capability and Gaps

CIV-MIL interaction is typically ad hoc in nature, with each military force attempting to establish their own information sharing process based on national policies and procedures. In a coalition with multiple military actors in theatre, coordination and de-confliction of military and civilian operations can be inefficient and unsuccessful resulting in an environment of distrust. Major shortcomings include:

- Military not understanding humanitarian community organizations, operations, culture, policies and purposes;
- Information sharing processes not standardized or supported by tactics, techniques and a procedures;
- Military use of classified systems for unclassified operations;

- Insufficient military personnel dedicated to performing the duty of releasing information to civilian actors, resulting in delayed information sharing;
- Military functioning as independent responders instead of coordinating with the affected state, other military organizations and humanitarian communities;
- Military responders not coordinating with one another and failing to achieve unity of effort and coherent shared awareness;
- Inability to share releasable portions of the common operating picture, including unclassified imagery and video;
- Lack of a CMIS strategy and lack of pre-deployment planning to include what information is needed, who has release authorization, and who needs the information, where, when, and in what form;
- Over-classifying information that could be released to the public (e.g. marking information with "For Official Use Only");
- Civilian actors not understanding the military structure, hierarchy, terminology or processes; and
- High turnover of military and humanitarian personnel in theatre, negating the value of already established information sharing processes.

1.3 Military Capability Development of CMIS

Currently military development of CIV-MIL capabilities is ad hoc. Improving processes and policies can be aided by employing the systems approach which requires capability developers to consider Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities, Policy, and Interoperability (DOTMLPF-PI).

1.3.1 Doctrine

- National doctrine should address CMIS as essential to successful humanitarian assistance across the spectrum of military operations.
- Doctrine should describe procedures for access by civilian liaisons to conduct coordination;
- Military organizations should establish information sharing processes that can allow sender anonymity and protect both the information source and recipient; and
- Nations should collaboratively develop a common standard for MNMCC roles, functions, missions and procedures.

1.3.2. Organization

- Enduring military operations require brining J9/CIMIC/CA capabilities within the structure to full effect in supporting the force commander and field staffs in navigating the CIV-MIL environment;
- The CMIS function must be fully integrated into command staffs, especially knowledge, information and data sharing and management plans and procedures;
- An information management and release procedures are needed at both the deployed staff and higher staffs wherever the release authority resides within the J9 structure;
- Release authority should be delegated to subordinate on-site commanders. A knowledge management capability is needed wherever the release authority resides; and
- Clearly define requirements and skill sets for military liaisons that represent the force at CIV-MIL coordination centers and other civilian locations.

1.3.3 Training:

- Train personnel in tactics, techniques, and procedures for CMIS;
- Training and education programs should include the understanding of:
  - Humanitarian community organizations
  - The principles governing the humanitarian community
  - Directives, both national and international, i.e. UN or treaty, governing interaction and operations;
- Train military personnel to not over classify documents that could be useful to civilian actors;
- Train personnel to be CIV-MIL liaisons; and
- Invite non-governmental, inter-governmental organizations (NGOs/IGOs) and other non-military organizations and agencies to participate in training, communication and command post exercises to both better understand their mission and expose them to military culture, organization and structure.

1.3.4 Materiel:

- Information gateway services should be included in mission networking capabilities to allow sharing of information between the classified mission network and the civilian entities operating on the public internet;
- Military liaisons working in civilian organizations should be given access to the mission network through mobile and portable devices; and

- Military networking environments need to connect to civilian information sharing tools (e.g. Google Docs and SharePoint).

1.3.5 Leadership

Leaders must gain experience operating in a CMIS environment, specifically:

- Commanders should gain experience or training integrating support elements (legal, financial, subject matter experts) to better enable CIV-MIL information dissemination;
- Military organizations should establish courses for leaders to learn about humanitarian missions, guidelines, and interaction with military forces based on the mission scenario;
- The importance of planning and preparation of CIV-MIL information sharing should be emphasized to and by leaders; and
- CMIS should be integrated into staff structures and the command battle rhythm.

1.3.6. Personnel

- Militaries must have an adequate number of personnel trained in information disclosure and declassification; and
- Militaries must have sufficient Public Affairs Officers to support the volume of information sharing needed to support CIV-MIL coordination.

1.3.7. Facilities

- Provide reasonable and convenient facilities to support CIV liaison activities in the military location to include communications support such as commercial phones and internet connections where necessary and feasible; and
- There must be adequate meeting/conference space to support unclassified CIV-MIL operations and briefings.

1.3.8. Policy

- Militaries should preplan common CMIS exchange requirements to ensure that information sharing is not delayed at the start of a mission; and
- Mission networking processes in FMN should include information release instructions.

1.3.9. Interoperability

- Structured information sharing via commonly prearranged formats and protocols, including formats in the FMN Joining, Membership, and Exiting Instructions for CIV-MIL information sharing should be promoted; and
- Common CIV-MIL data exchange formats based on open, public standards should be used as much as possible.

SECTION 2: OPERATIONS AND SUPPORT

2.1 Missions

This section of the Operational Concept describes the three distinct CIV-MIL use cases: cooperation, de-confliction, and coexistence. These environments will influence what and how information is shared and the level of trust that can be expected between information sharers.

Trust in the humanitarian context is risk to the organization's ability to access the affected population, including physical risk to the affected population and their field staff. Trust can also be based on organizational policy or personal experience.

Figure 4 depicts the spectrum of coordination overlaid against the three CIV-MIL environments (cooperation, de-confliction, coexistence).

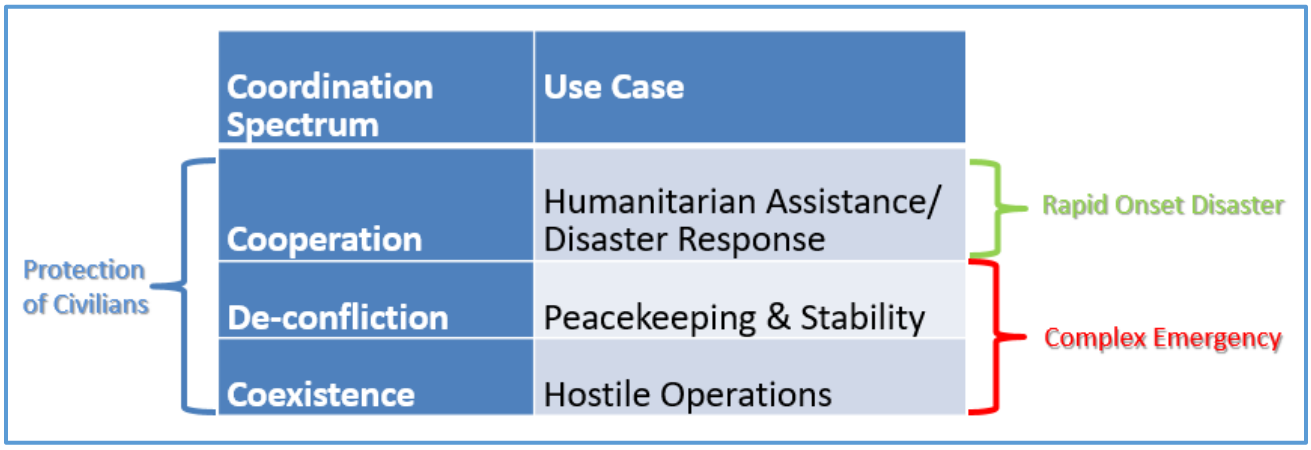


Figure 4

2.1.1 Cooperation is an environment where trust is high between most CIV-MIL participants, such as during a humanitarian assistance/disaster response mission. In a cooperative environment the military's role is to support humanitarian operations by providing unique capabilities that are not available to the civilian actors or to provide a rapid response force during the initial stages of the event. To be effective the military and the civilian actors need to interact closely, sharing information and situational awareness, and coordinating operations. In this environment CIV-MIL collaboration, cooperation, and coordination is at its highest since the CIV-MIL goals should align and be mutually supportive.

2.1.2 De-confliction is an environment that is more restrictive than the cooperative environment but less restrictive than coexistence. In a de-confliction environment information sharing should be aimed at optimizing the overall strategic objectives of the mission, both military and civilian. The level of interaction between civilian and military actors will depend upon and the level of trust that exists. The de-confliction environment is often found in peacekeeping and stability operations where sustained combat operations have been completed and are not anticipated. The military role will be to enable humanitarian operations while having limited participation in those operations. Interaction between civilian and military actors may be overt and include meetings and liaison exchange.

Be aware that the term de-confliction can have divergent meanings to civilian and military personnel. The civilian interpretation is deescalating a conflict. The military interpretation is avoiding actions that interfere with the other entities mission, where possible, especially those which might endanger non-combatants. For the purposes of this document we employ the military interpretation of de-confliction.

2.1.3 Coexistence is an environment featuring hostilities or complex operations in which the military conducts combat operations while the humanitarian community is engaged in supporting the affected population. In this environment trust between civilian and military actors is low and the majority of the humanitarian community will likely distance themselves from direct contact with the military. Within this environment information sharing needs to be focused on avoiding friendly and neutral casualties, establishing humanitarian space and ensuring independence of civilian actors. Threat to humanitarians or the affected population is a primary information sharing consideration.

2.2. Stakeholders

It is important to identify the main participants and their role in an operation/response. The three primary stakeholders in CMIS are the affected state, the humanitarian community, and the military. Foreign government agencies and host nations may also be included as stakeholders.

2.2.1 Affected State

The affected state is the sovereign government. This term includes national and regional governments and associated departments and ministries. The affected state ultimately has responsibility to support and protect the population, however, it may

not be capable of providing such support and protection. In this case, CMIS information sharing will become particularly critical.

National sovereignty must be observed throughout an operation. Foreign military forces operate with permission of the affected state. The authority (actual or perceived) of the affected state must never be infringed upon during operations, including observance of state laws, regulations and customs. Foreign governments may advise the affected state, however, ultimate authority resides with the affected state's government.

2.2.2. Humanitarian Community

This community consists of independent international and local, mostly non-governmental, organizations that strive to reduce suffering, save lives and improve the health, education, and life of a population. These actors are independent and are accountable to the affected state, the population they support and their own management.

2.2.3. Foreign Military

These are armed forces or civil defense forces under the control of their national government. These actors conduct operations in support of their national policy. They may be organized as a coalition or operate independently. They may employ a mission network as an enabler of communications and coordination even when a coalition or multi-national force is not present.

2.2.4. Foreign Government Agencies

Agencies of foreign governments may be engaged in a mission area. These actors may include the diplomatic representatives from the responding nations' governments.

2.2.5. Host Nation

Either due to limited access to the affected state, or the need to have logistic hubs outside the affected state – basing for the military operation outside the affected state may become necessary. States which provide access for this purpose are host nations.

2.2.6. Development and Reconstruction Community

Specialized activity in developing or post-conflict areas focused to establishing the rule of law, political governance, economic rehabilitation and development, and social conditions such as justice and reconciliation. The effort may include distribution of

relief assistance, restoration of infrastructure, and reestablishment of social services to facilitate private sector development, structural reforms for stability and sustainable growth.

2.3. Assumptions and Constraints

2.3.1. **Assumptions**

Assumptions enabling information sharing include:

- Members of the responding military will establish a Mission Network;
- CMIS will be needed to conduct operations; and

2.3.2. **Constraints**

The authority to share information is based on national policies and includes restrictions on sharing. The specific information that can be shared and with whom will be situationally dependent based on the mission type, the affected state condition (failed, weakened, totalitarian, monarchal, constitutional democracy) and the level of interaction between the military and the civilian community.

2.4 Capability Description

Responding multi-national military forces form an FMN environment for sharing information among the military participants. A key element of FMN is the set of instructions for joining, membership, and exiting the network. FMN participants will use these instructions to establish, maintain and disconnect from the federated network. The civilian community is not expected to join the FMN environment, but non-FMN entities will share information by other means including internet websites, email with attachments, voice and text, bi-lateral cross-domain gateways and face-to-face conversations. It is important to note that liaisons can provide face-to-face connection between military and civilian actors that supports trust, interaction, and understanding.

2.5 CMIS Employment in FMN

When a federated mission network is created, it will be protected at an appropriate classification level. To enable CMIS, the FMN environment must include **an unclassified space with connectivity to the public internet.** The flow of information from the classified mission network to the unclassified space and vice versa must be controlled to ensure public release policies are followed. In a cooperative environment information dissemination between the FMN participants and civilian actors can be direct. In low-trust coexistence environments, the information flow tends to be

through a third party, i.e. an interlocutor. Information sharing in the de-confliction environment may require direct or third part information flows depending on the nature of the mission and relationship between civilian and military actors.

2.6 Potential Impacts of CMIS

CMIS is not a new concept. The new element to this existing concept is the introduction of FMN as a coalition networking capability that has common procedures and standards. The net result of FMN-enabled information sharing among members and non-FMN mission actors will be positive. FMN-enabled information sharing with civilian actors will increase unity of effort and reduce friction by facilitating coordination and cooperation among parties.

SECTION 3: USE CASES/SCENARIOS

3.1 Operational Scenarios.

This Operational Concept will be presented using three Use Cases based on the level of information sharing anticipated between the military and civilians in the environment (Figure 5). The range of information sharing extends from 'cooperation' where for a majority of the CIV-MIL entities trust is high and information sharing is extensive. Environments where trust is low for the majority and information sharing is limited to only the essential required is represented by 'coexistence'. Between the two extremes, the Operational Concept recognizes the middle ground, 'de-confliction', which may be a peacekeeping and stability operational environment that could dictate the level of CIV-MIL interaction. (FMCM Use Cases are explained in detail in the FMCM Guidebook, Enclosure 3.)

Information sharing between appropriate IO/NGO community, affected state and military actors may include:

- Planning information focused on future operations and long term objectives;
- Security information: information relevant to the security of both staffs (military and civilian) and the population at risk in the area of operation;
- Humanitarian locations: the coordinates of humanitarian staff and facilities inside military operating theatre;
- Humanitarian activities: the humanitarian plans and intentions, including routes and timing of humanitarian convoys and airlifts, to coordinate planned operations while simultaneously avoiding accidental engagement or interaction with humanitarian operations;
- Mine-action activities: information relevant to threats or current mine activities;
- Population movements: information on major movements of civilians;
- Relief activities of the military: information on relief efforts undertaken by the military;
- Post-strike information: information on strike locations and explosive munitions used during military campaigns to assist with the prioritization and planning of both humanitarian relief and mine and unexploded ordinance removal activities.

In all three scenarios the resources, capabilities and information users are the same. The differences in the scenarios are what is shared, who it is shared with, and how it is

shared. Besides the level of coordination, there are other factors affecting civilian organizational willingness to share information or even interact with foreign military forces. These include:

1. Overall outlook of the organization towards interacting with foreign military forces.
2. Determining if interacting with foreign military forces enables operational benefits for access and security in providing relief to the affected population.
3. Determining if interacting with foreign military forces will negatively affect their relationships with parties in other conflicts where the agency is working to project a credible image of neutrality and impartiality.

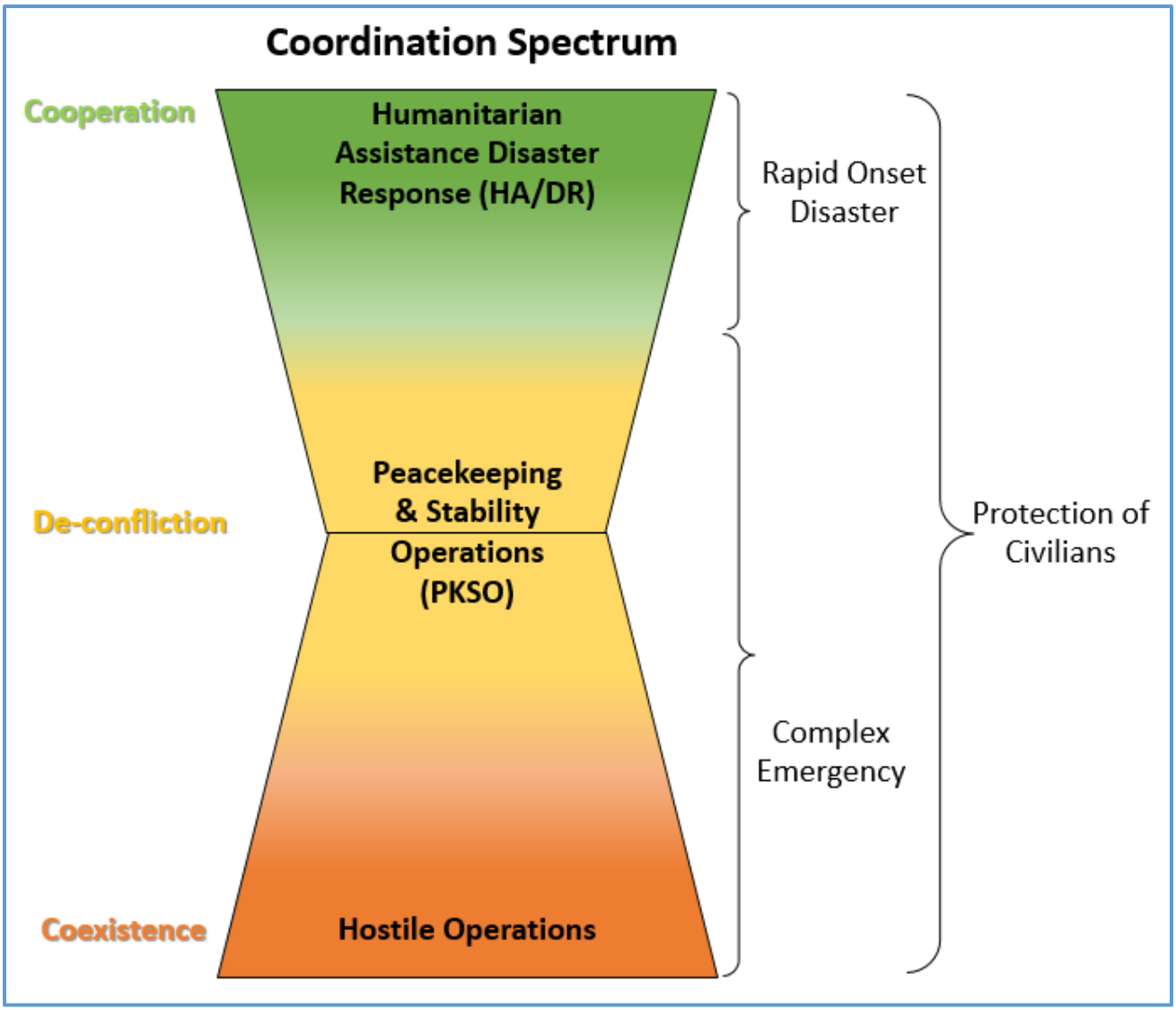


Figure 5

3.2 CMIS Operations Use Cases

3.2.1 Cooperation: This scenario represents a high potential for information sharing among all participants (civilian, military, affected state government). This is often found in a rapidly unfolding disaster in a benign enemy threat environment. In such a scenario, critical information needed would include how the disaster affected existing physical infrastructures, along with the affected population's immediate needs such as food, shelter, medical care, sanitation, etc. Information will need to be gathered (and shared) as quickly as possible. The Cooperation environment often contain the following assumptions:

- Due to the compatible objectives, coordination, collaboration, and cooperation are high among the participants (military, affected state government, humanitarian community).
- Trust is high if allowed by the organization's policy since the CIV-MIL association risk to the humanitarian staff and the affected populace is low.
- High level of direct communication between all the parties, through either face-to-face meetings, text messages, or emails with attachments, etc.
- Military units are usually more willing to share information derived from sources (classified and unclassified) to support ongoing relief operation.
- The humanitarian community is more willing to accept military assistance (logistics support, materiel movement, engineering support, etc.).
- Participants are willing to provide and accept liaisons as requested in order to facilitate planning.
- Even in a cooperative environment, organizations will still take steps to maintain independence and neutrality so misperceptions are not spread via social media which can affect their effectiveness and safety in other places.

3.2.2 De-confliction: This scenario represents the area between the extremes of "cooperation" and "coexistence." Information sharing is based on the level of interaction between the CIV-MIL participants in an environment often characterized by limited hostile engagements and where sustained combat is not anticipated. This is common in PKSO missions. The military may have a role in providing a secure environment for humanitarian operations while not directly participating in the humanitarian operation. Any interaction between CIV-MIL individuals or groups may be low key and conducted in an independent setting not associated with either party if needed to establish trust and minimize the risk to PKSO participants. Though the CIV-MIL entities have different tasks, the overarching military goal of stability and the civilian (humanitarian) goal of recovery are inextricably linked requiring

flexibility and adaptation to overcome aforementioned common individual organizational information sharing constraints. This environment commonly contains the following assumptions:

- Coordination, collaboration, and cooperation are conducted at appropriate level agreeable to engaged CIV-MIL entities based on the possible mix of de-confliction and coexistence as the situation dictates. Information sharing may be limited to establishing situational awareness for example using a common operating picture concerning threats and location of humanitarian operations.
- In order for the humanitarian community to demonstrate independence, communication with the military maybe conducted either at an independent location or through a trusted third party such as an interlocutor.
- The military is less likely to share information concerning ongoing or future operations, but may be willing to share more non-tactical information such as weather and past insurgent activity that is no longer of tactical utility.
- Military sharing of information with the humanitarian community about adversary activities during a conflict would contribute to maintaining the safety and security of humanitarians and the affected population.
- Web-based (i.e. portals and email) information dissemination are tightly controlled with very limited access by participants, and may be read-only to give anonymity to the source material provider. This protects both the sender and receiver from attribution if the information is disclosed to a hostile force.
- Liaison personnel to de-conflict operations are used as needed or requested.

3.2.3 Coexistence: This scenario is the other extreme of the information sharing with minimum open sharing of information and is often found in hostile environments involving combat operations. In such an environment, trust is often low as major CIV-MIL participants strive to provide safety for their specific communities of interest. Their goals often may not coincide with those of other major participants. Absent a shared mission, these participants coexist yet seek to avoid direct interaction and contact in order to project independence. This environment commonly contains the following assumptions:

- Coordination, collaboration, and cooperation are restricted to only the degree that will not negatively affect operations.
- Humanitarian communities guard and assert their independence by rarely communicating directly with military organizations.
- Much, if not most, information sharing will be built on existing personal and institutional trust.

- The military is less likely to share operational information but may be willing to share information that is no longer of tactical utility, like weather and past insurgent activity, along with a common operational picture for situational awareness.
- To maintain independence the humanitarian community will most likely decline military assistance and avoid any appearance of cooperation with military forces.
- Web-based (i.e. portals and email) information dissemination are tightly controlled with very limited access by participants, and may be restricted to read-only to give anonymity to the source material provider. This protects both the sender and receiver from attribution if the information is disclosed to a hostile force.
- Participants utilize interlocutors in order to facilitate de-confliction.

SECTION 4: FUNCTIONAL CAPABILITIES

Tools to affect information sharing in an unclassified CIV-MIL environment are:

- Voice – this can include land lines, cell phones, and voice over internet protocol (VoIP);
- Text – commonly associated with smart phones but can be internet-based;
- Email – internet mail with supporting software like Microsoft Office products (Word, Excel, PowerPoint) and Adobe PDF files;
- Video Teleconferencing – Similar to VoIP, video and audio are shared between parties;
- Face-to-Face – improves trust and discussions amongst participants;
- Internet posting and access to upload/download information accessible by specific individuals with controlled access or shared with the public without access control;
- Readable databases that can be accessed by specific individuals with controlled access, or shared with the general public without access control; and
- File sharing with access control.

5.0 APPENDICES

5.1 Glossary of Terms and Acronym Listing:

Term	Acronym	Definition
Coexistence		In events with high physical threat and/or low trust CIV-MIL entities avoid direct interaction and contact in order to project independence.
Cooperation		CIV-MIL environment common in low threat environment and high levels of trust commonly associated with high amounts of information sharing and direct interaction between the two entities.
De-confliction		1. To adjust or coordinate so as to prevent or resolve conflict and avoid a potential problem or accident involving activities by two or more entities in a particular combat area. 2. De-confliction environment represents the level of information sharing that falls between the cooperative direct support state and the no-contact coexistence state. This environment commonly occurs in post conflict peacekeeping
Direct Support		The military direct support role is to support the relief mission by providing unique capabilities that are not available in the civilian environment or to serve as a rapid response force to provide the initial capability while the civilian response is deployed. The key attributes in this environment are that the military is in support to the relief effort and is the resource of last resort to provide support capability to the overall HA/DR effort.

Term	Acronym	Definition
Doctrine, Organization, Training, materiel, Leadership & education, Personnel, Facilities, Policy, and Interoperability	DOTmLPF-PI	A capability development system that parses requirements into discrete elements required to effectively introduce changes to systems or organizations.
Federated Mission Networking	FMN	A capability consisting of three components: (1) Governance (2) a management framework and (3) mission network instantiations in a mission or exercise. Also considered the best means to create a common, mission-wide data and information sharing environment.
Federated Mission Networking/Mission Partner Environment Civilian-Military	FMCM	A FMN/MPE framework which supports and enables the planning and execution for the timely establishment of effective information sharing, cooperation, coordination, and collaboration with non-military entities across the range of Civilian- Military operations, including support of sudden onset disasters.
Foreign Government Agencies		There will be other agencies of the government engaged in the response effort beyond their military. This normally will include the diplomatic representatives in country and other agencies of the foreign office/state department of the responding nation's government.
Foreign Military		These are commonly armed forces under the control of their national government's authority and conduct operations supporting its national policy. Military forces can be grouped as a coalition or might operate as independent entities based on their respective national directives and policy.

Term	Acronym	Definition
Host Nation	HN	A nation which, by agreement: a. receives forces and materiel of organizations or other nations operating on/from or transiting through its territory; b. allows materiel and/or military organizations to be located on its territory; and/or c. provides support for these purposes.
Humanitarian Assistance	HA	
Humanitarian Assistance/Disaster Relief	HA/DR	
Humanitarian Community		There are a myriad of organizations, large or small, that conduct operations intended to reduce suffering, save lives, and improve the health, education, and life of a population. Humanitarian communities are a collection of independent organizations. They associate to collaborate, cooperate, and coordinate when it is in their best interest to do so – otherwise they are fully independent organizations only accountable to the affected state and their own management.
Humanitarian-Military Operations Coordination Center	HuMOCC	Serves to provide a predictable humanitarian-military and police coordination platform. It provides the physical and virtual space for facilitating the interface among humanitarian actors, national and foreign military actors, and the country's national police.
Humanitarian Principles		Foundation for humanitarian action include four humanitarian principles: humanity, neutrality, impartiality and independence. They are central to establishing and maintaining access to affected people whether in a natural disaster or a complex emergency, such as armed conflict.

Term	Acronym	Definition
Information sharing		The conveyance of information to include data, particularly structured data, between civilian and foreign military entities to include humanitarian community and the affected state central and regional governments and their military.
Interlocutor		A third party person or organization who can be utilized as a conduit for information sharing or to help provide interaction between military and humanitarian actors,
International Federation of the Red Cross and Red Crescent Societies	IFRC	
International Non-Governmental Organization	INGO	Legally constituted corporations created by natural or legal means that operate independently from government. The term normally refers to organizations that are not a part of a government and are not conventional for-profit businesses.
International Organization	IO/IGO	An intergovernmental, regional or global organization governed by international law and established by a group of states, with international juridical personality given by international agreement, however characterized, creating enforceable rights and obligations for the purpose of fulfilling a given function and pursuing common aims
Joining, Membership, and Exiting Instructions	JMEI	Method and process for military information systems to form a unique network environment, exchange information and then disengage in an orderly manner.
Knowledge Management	KM	Information results from the processing of raw data. Knowledge management is getting the right information to the right person at the right time and in a usable form.
Liaison Officer/Official	LO	Military term is Liaison Officer, civilian equivalent is Liaison Official.

Term	Acronym	Definition
Military and Civil Defense Assets	MCDA	
Mission Partner Environment	MPE	An operating environment that enables Command and Control (C2) for operational support planning and execution on a network infrastructure at a single security level with a common language.
Multi-National Coordination Center	MNCC	
Multi-National Military Coordination Center	MNMCC	
Non-Association		In environments with low CIV-MIL trust, humanitarian entities may distance themselves from the military. This is necessary to present and maintain independence in all aspects of their operations.
Non-Governmental Organization	NGO	A private, self-governing, usually non-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society.
Operational Concept		Describes how selected capabilities are employed to achieve desired objectives or end-states for a specific scenario.
Public Affairs Officer	PAO	Element of a military organization designated to support media engagement on behalf of the military.

Term	Acronym	Definition
Tactics, Techniques & Procedures	TTP	
United States Agency for International Development	USAID	
Voice Over Internet Protocol	VOIP	

5.2 References –

A. NATO Federated Mission Networking, Implementation Plan Volume I, FMN Implementation Overview, dated 11Aug14.

B. Future Mission Network (renamed Mission Partner Environment) Initial Capability Document (ICD), dated 22Dec11.

C. Future Mission Network (renamed Mission Partner Environment) 90-Day Study, dated 17Dec12.

D. Mission Partner Environment Tier 1 (Enduring) Capability Definition Package, dated 21Apr14.

E. Unclassified Information Sharing Service Internet Services Public & Private Capability Packages, dated 15Dec14.

F. Episodic Mission Partner Environment Capability Definition Package, dated 23Mar15.

G. UN CMCoord Field Handbook
https://docs.unocha.org/sites/dms/Documents/CMCoord%20Field%20Handbook%20v1.0_Sept2015.pdf

H. UNHCR and the Military – a Field Guide
http://www.refworld.org/docid/465702372.html

I. ***IASC Reference Paper on the Civil-Military Relationship in Complex Emergencies***
http://www.refworld.org/docid/465702372.html

FMCM Project Lead: Charles (Bill) W. Robinson, United States Joint Staff J7, Suffolk, VA, charles.w.robinson20.civ@mail.mil .


MCDC
Multinational Capability Development Campaign