Annual CIMIC Foresight Conference 2024

Reporting the outcome

EXECUTIVE SUMMARY

The Annual CIMIC Foresight Conference 2024 (ACFC24), hosted jointly in The Hague from October 7th to 11th by the Civil-Military Centre of Excellence (CCOE) and NATO Supreme Head Quarters Allied Powers Europe (SHAPE), successfully brought together civilian and military experts with the intent of questioning and shaping the future of Civil-Military Cooperation (CIMIC). By addressing the complexities of both current and future operating environments, the conference positioned CIMIC as a pivotal military joint function but highlighted the need for clarification of its capabilities in times of peace, crisis, and conflict.

The report aims to provide a comprehensive overview of the discussions and outcomes of the Annual CIMIC Foresight Conference 2024 (ACFC24). It seeks to capture the insights and recommendations generated during the conference, mainly focusing on enhancing CIMIC capabilities to address current and future security challenges.

SETTING THE SCENE

ACFC24 was a dynamic event aimed at addressing the complexities of the current and future operating environment and its implications for CIMIC. The conference focused on integrating civil-military perspectives across various sectors to enhance CIMIC's future readiness.

ACFC24 attracted 150 participants (Annex 1) from over 30 nations, achieving a balanced representation of military personnel and civilians from academia, the humanitarian sector, and private organizations. This diverse audience contributed to a rich exchange of ideas and insights, demonstrating the high level of engagement and willingness to collaborate within the CIMIC community and its partners.

In line with the warfighting imperatives outlined by the NATO Warfighting Capstone Concept and Warfare Development Agenda, the conference covered five main topics for working groups:

- The understanding of the current and future operating environment (related to: **Cognitive Superiority**);
- Resilience from military and civilian perspectives, including Domestic CIMIC (related to: **Layered Resilience**);
- Shaping the operating environment from a human security perspective (related to: **Influence and Power Projection**);
- CIMIC's future role in a Multi-Domain environment (related to: **Cross Domain Command**);
- The current and future threat landscape and its implications for CIMIC (related to: **Integrated Multi-Domain Defence**).

The conference agenda included keynote speeches to set the tone for the working group topics, followed by a Q&A panel discussion that engaged with the keynote speakers. The participants were divided into five working groups, one for each topic, led by experts both from academia and the military. These sessions facilitated focused discussions, merging and confronting the attendees' perspectives to conduct a gap analysis identifying areas for further development of CIMIC capabilities. The results of these working sessions were presented to a panel of experts, providing a platform for attendees to share their findings, learn from others, and gain a deeper understanding of the field's complex challenges. The panellists complemented the gap analysis with their expertise and highlighted the importance of defining a clear set of CIMIC capabilities to address the fast-paced evolving security landscape with a focus on human-centred strategies.

Understanding of the current and future operating environment

The future operating environment is characterized by increasing uncertainty and complexity, which emphasizes the critical importance of fostering trust among all actors involved in or affected by military operations. In efforts to anticipate future scenarios, group discussions highlighted several potential risks, including climate-induced migration, global security fragmentation, and conflicts on multiple scales. These challenges could:

- lead to either isolation or cooperation,
- trigger escalating resource disputes,
- and increase technological dependency.

The growing use of disinformation in information warfare exacerbates these dynamics. It threatens to weaken or even dismantle the trust between civil and military actors.
The working group identified key challenges, particularly the necessity of preserving trust and mutual understanding, as hybrid warfare -especially information warfare- seeks to erode these bonds. That includes significant and dangerous threats, such as concurrent conflicts, hybrid warfare, and the potential weaponization of natural disasters and migration. Based on a military design thinking approach[1] the recommendation is:

- to foster a mindset of readiness and resilience among all stakeholders and enhance CIMIC capabilities through focused training exercises,
- community and network-building initiatives,
- pre-planning efforts,
- and sharing situational awareness and understanding.

Additionally, the working group stressed the importance of establishing clear mandates and tasks for ongoing daily engagement with key actors. Such interactions will promote mutual understanding and network development, ensuring a unified and coordinated response to future challenges on a larger and more complex scale.

[1] to address these issues, initially exploring and defining the problem space before progressing to solutions that targeted the core issues.

For CIMIC to effectively navigate the complexities of future operating environments, robust analytical capabilities that integrate technological advancements are required. This involves:

- a deep understanding of the civil factors of the operating environment, including
- social, technological, political, economic, and ecological factors that shape the landscape of military operations (context),
- the ability to interpret current data and trends to foster trust and cooperation between military and civil actors (insight),
- the capacity to anticipate future risks and challenges, such as technological dependencies and hybrid warfare,
- and to plan accordingly (foresight).

Technological advancements can significantly enhance CIMIC's analytical capabilities, enabling better situational awareness, faster information sharing and improved decision-making processes. Artificial intelligence, for example, not only enhance the spread of disinformation through sophisticated content generation and distribution algorithms but it can also provide advanced tools for detecting false information and verifying facts efficiently.

These advancements are critical for providing a comprehensive understanding of the future operating environment desperately needed in all kinds of operations.

Resilience from military and civilian perspectives and domestic CIMIC

This working group allowed participants to explore the importance of societal resilience, the roles of civilian actors in supporting military efforts, and the need to define domestic CIMIC in a NATO context. The session was structured around a guiding question: What minimal boundary and framework conditions in the civilian environment are necessary to make military operations possible and meaningful?

Through a structured five-step facilitation approach[2], participants were guided to analyse the interconnectedness between the different actors related to resilience and CIMIC from national to regional and supranational levels. The group discussed the CIMIC principles and practices in various operational contexts, including domestic and expeditionary scenarios. A focus was placed on sub-article V situations, emphasizing the need to clarify responsibilities and authorities and understand financial relations, contracts and agreements.

It was agreed that the early integration of local authorities in the planning process is vital, with trust being a fundamental factor in facilitating effective information sharing, cooperation, and interoperability. The main gaps highlighted the need for improved general foresight and alignment with external actors. Conceptual ambiguities were pointed out between national and NATO CIMIC frameworks and insufficient civil-military synchronization efforts – particularly concerning infrastructure and the cyber domain.

[2] The five steps included: Identification of relvenat actors through a PMESII Matrix; mapping interdependencies between actors; integrating civil factors within several sectors; analysing civil-military interaction; identification of influencing factors on military and civilian activities.

A decline in social cohesion - exacerbated by increasing individualization - further undermines societal resilience - worsened by hybrid activities such as disinformation campaigns.

The key takeaways from the discussions within the group are:

- that success ultimately depends on the right people with the right understanding and skills. It is essential to attract talented and committed personnel, raising the question of whether the military context remains sufficiently attractive.
- There is also a significant lack of knowledge between private, public and military partners about each other's capabilities and procedures. Early integration of civilian partners into the planning processes, alongside formal agreements and joint emergency frameworks, is essential.
- Lastly, data sharing emerged as the most critical gap. Digital interoperability remains underdeveloped, and establishing data-sharing standards will require technical solutions and a shift in mindset.

Addressing the identified gaps in personnel attraction, inter-sector knowledge, and data sharing is crucial for enhancing operational effectiveness and resilience. By fostering an environment that attracts skilled individuals, promotes mutual understanding among private, public, and military partners, and prioritizes the development of robust digital interoperability standards, preparedness and response capabilities can be significantly improved.

Shaping the environment from a human security perspective

The working group explored how the future security landscape will influence the conceptualization and implementation of human security through 2030 and beyond. Emphasizing NATO's 360-degree approach, the group identified key threats to human security and highlighted the importance of 'strategic empathy' in understanding others' needs and perceptions. As urban warfare becomes more prevalent, incorporating human security considerations is essential for NATO to distinguish itself from adversaries who target civilians during conflicts either without any discrimination or, as could be observed in the recent Ukraine war, deliberately as primary target.

While protecting civilians (PoC) is a priority and moral imperative, human security encompasses much more and constitutes a mandatory policy in NATO. The discussion highlighted the need to shift from traditional state-centric paradigms to a more holistic approach that prioritizes the safety and well-being of populations. Human security is central to mission success, with the military as a deterrent against threats across multiple domains and a supporter of civilian resilience. The role of CIMIC in orchestrating information gathering was highlighted, along with the need for standardization across NATO to ensure a cohesive approach.

However, the group highlighted the need for clarification regarding the role of CIMIC in human security and its integration within the overarching civilian environment. Promoting long-term, sustainable peace, security, and stability is best achieved in cooperation with the local authorities, population, and civil society. Security is about military capabilities and the underlying social, economic, and political factors contributing to it.

The team advocated for incorporating civilian primacy in national defence approaches, following the principle of "as civilian as possible - as military as necessary." To effectively implement human security, it is crucial to understand how different actors conceptualize it, which involves comprehending the system and interactions between stakeholders. In the context of CIMIC, power projection should begin by learning about others and understanding how to work collaboratively.

The working group proposed that human security should be recognized as a joint function, with CIMIC serving as a key enabler since it is the main area where all human security topics come into play. Strengthening CIMIC capabilities, particularly for protecting civilians, will enable the Alliance to better protect its human capital in the short and long term.

CIMIC's future role in a Multi-Domain environment

The CIMIC community is transitioning alongside with the other military functions from focusing on Crisis Prevention and Management to NATO's Core Task of Deterrence and Defence, driven by the evolving geopolitical landscape. This shift necessitates a mindset change across societies and militaries, emphasizing readiness for NATO's Command and Force Structures. The role of CIMIC in Multi-Domain Operations (MDO) is increasingly vital, as this concept inherently involves the synchronization of military and non-military activities to achieve the desired converging effects. CIMIC is fundamental to comprehensively understanding the operational environment through Civil Factor Integration (CFI) and Civil-Military Interaction (CMI). This approach applies across all five domains, particularly in cyberspace, arguably the most civilian-oriented domain alongside space. In cyberspace, CIMIC must collaborate with a wide range of stakeholders to provide crucial analysis and understand the unique capabilities they bring, which are often absent in traditional military contexts. Next to that, to enable, reinforce, and sustain operations in all military domains, close cooperation with civil society is essential. As NATO increasingly relies on non-military actors (and their capabilities), CIMIC's value lies in analysing civil actors' roles, bridging military and civilian sectors, and facilitating civil factor integration. This analysis is essential for integrating the unique factors emerging from cyberspace and mitigating complexity through a structured, collaborative approach, which is crucial for mission success in peacetime, crisis, and conflict. A subsequent step would involve developing a matrix that delineates which military entities coordinate with specific civilian entities to enhance clarity and streamline collaboration.

The working group highlighted the difficulties in finding a common understanding of the role of CIMIC in MDO. The problems seem to arise from the lack of general knowledge and understanding of the concept and finalised documents on the NATO MDO topic as well as the still diverse attempts to operationalise this concept. Also, the synchronization efforts on the different levels (strategic-operational-tactical level) are not apparent at this point, making it hard to envision the role and responsibilities of CIMIC and CIMIC staff in this. Through reverse engineering and real-life examples, the participants highlighted that CIMIC's involvement spans three effect dimensions: physical, cognitive, and virtual. The crucial role of CIMIC begins at the scenario's outset, where it analyses the civilian context around an incident, such as a bridge's destruction, and assesses its importance to the local area through Civil Factor Integration.

This involves analysing potential impacts on the local population by analysing possible second and third-order effects and has implications across domains:

- air (destruction),
- cyber (surveillance and sabotage),
- and land (psyops and engineering).

Effective CMI in each domain requires coordinated information sharing, collaborative assessments, and cooperative defence strategies to protect critical infrastructure, ensure cybersecurity, and respond to threats. While traditional domains are more mature and better understood, CIMIC must leverage civilian expertise and resources and develop domain-specific capabilities, considering that MDO depend on every single domain. Still, every domain can also be in an enablement role for the other. Ultimately, it became clear that sharing knowledge and perspectives helped the participants better understand what MDO is and is not.

The current and future threat landscape and its implications for CIMIC

In the evolving threat landscape, NATO faces multifaceted challenges characterized by Russia's influence abroad like in Africa, mounting pressure on the Alliance southern flank, the strategic threats posed by China's economic influence and resource dependency, and emerging threats from the Eastern Flank.

Russian Private Military Companies' (PMCs) influence in Africa exemplifies the complexity of emerging threats that NATO needs to consider in its 360-degree approach. These PMCs support Russia's ambition to reassert itself as a superpower by using soft power to counter Western influence. The strategic implications for NATO are profound, as PMCs increase migrant flows, destabilize local governance, and amplify Russian disinformation campaigns in Africa, all of which necessitate a coordinated and robust response from the Alliance. The threat landscape is further complicated by emerging challenges from the Eastern Flank and China's strategic manoeuvres. Sub-threshold threats such as cyber-attacks, disinformation, and territorial incursions require NATO to enhance its deterrence and information management capabilities. China's economic influence and technological advancements, outreach into the international system -like the establishment and strengthening ofb the BRICS union - coupled with its strategic partnership with Russia, underscore the need for NATO to adapt its CIMIC strategies to ensure resilience and operational effectiveness.

The working group identified several critical areas for improving CIMIC, including:

- integrating the joint function Information by involving, liaising and coordinating CIMIC Staff within the broader INFO OPS-community,
- reducing decision-making time,
- and efficiently allocating surge capabilities like human resources and finances,
- lack of standardized operating procedures, structures, and training further impedes effectiveness.

CIMIC must improve communication and coordination with key actors in energy and cyber security and access financial experts. Proposed solutions include:

- securing freedom of movement in the Schengen Areas without any interference by establishing long-term contracts with logistic companies;
- establishing NATO Marshall forces for food distribution and protection upon nation request to ensure protection of the food security process, supply chain and critical infrastructure;
- ensuring CIMIC Liaison Officers are effective links between military and host nations developing situational awareness to advise commanders and effectively engage with the joint function Information;
- developing a Surge Capability Doctrine as a framework designed to rapidly increase CIMIC Operational Capacity in response to crises aimed at effective resource mobilization and flexible deployment.

Allied countries should focus on preparedness training and community building to enhance agility and technological superiority. The group also stressed integrating CIMIC into manoeuvres, which is currently hindered by language differences within the Alliance and unclear mandates. Understanding organizational roles is crucial for effective responses, and deploying more full-time functional specialists will ensure NATO's strategic agility in addressing complex threats.

Gaps and conclusions

Combining the results from the working groups and the final panel discussions, it is evident that, as we look to the future, CIMIC is not expected to diminish; instead, it must evolve and expand in response to emerging drivers and trends in the future operating environment. The conference's primary aim was not to devise solutions but to identify the significant gaps in CIMIC that need addressing to ensure its future readiness. Key findings were categorized according to the Warfare Development Agenda's critical enablers: People, Data, Technology, Agility, Integration, Preparation, and Interoperability.

Among these, people were identified as the most critical enabler, emphasizing the need for military operations to focus on the human aspect, which is integral to various joint functions, including CIMIC. CIMIC contribution to Human Security needs to be clarified, adopting a holistic perspective to ensure the effective use of the Military Instrument of Power. People also refer to the need to attract and develop the proper skill set to effectively understand the complexities of the current and future operating environment. Building trust and understanding between civil and military sectors through ongoing engagement is vital.

Regarding data, better alignment and information flow between national and multinational entities are required to synchronize domestic and NATO CIMIC efforts. While technology enhances CIMIC's mission efficiency, it cannot replace human interaction or build trust, highlighting the need for a balance between innovation and human-centred strategies. Integration challenges were noted, particularly in achieving a shared understanding of Multi-Domain Operations.

CIMIC must clarify its domain-specific capabilities while ensuring a comprehensive understanding of the civil factor of Multi-Domain operations and inter-domain effects. Preparation involves reviewing CIMIC capabilities for readiness and geographical specialization, defining capabilities that enhance resilience and determining domestic CIMIC requirements.

The path forward for CIMIC within NATO requires a strategic approach that integrates both traditional and innovative methodologies to enhance its effectiveness in a complex operational environment. The NATO CIMIC Centre of Excellence has identified 6 main areas of development for addressing the above-mentioned challenges:

1. **Adopt a standard definition of domestic CIMIC** to clarify requirements for domestic CIMIC within the NATO context and define clear roles and responsibilities.
2. Beside standardised cross domain CIMIC basics the **development of domain-specific CIMIC capabilities** in dialogue with other NATO agencies and civilian partners.
3. **Operationalization of MDO concepts**, clarifying CIMIC role beyond humanitarian actors' engagement, which include
    a. Analysing and assessing civil factors in the operating environment.
    b. Synchronizing military and non-military activities, especially in space and cyberspace domains.
4. **Define the Military Contribution to Human Security** in dialogue with other NATO agencies and civilian partners.
5. **Review CIMIC capabilities** through experimentation and evaluation of new technologies, such as Artificial Intelligence, to enhance analysis and assessment.
6. **Continue the Annual CIMIC Foresight Conference series** to address specific gaps and brainstorm standard solutions.
7. **Expand the CIMIC roadshow** to the non-CIMIC community, including military personnel.

ANNEX 1. Participating Organisations

Universities and Research Institutes

1. Canadian Defence and Security Network
2. Centre for International and Defence Policy (CIDP) / Queen's University
3. Clingendael Institute International Relations
4. DCAF- Geneva Centre for Security Sector Governance
5. Delft University of Technology
6. Dublin City University
7. EPIS ThinkTank e.V.
8. European Council for Foreign Relations
9. Helmut Schmidt University
10. Hochschule des Bundes für öffentliche Verwaltung (HS Bund), Federal University of Administrative Sciences
11. International Centre for Policing & Security, University of South Wales
12. Joint Civil-Military Interaction Network/Middle Georgia State University
13. National Defense University Carol I - Regional Department of Defense Resources Management Studies, Bucharest
14. Ostbayerische Technische Hochschule Regensburg
15. Royal Danish Defence College
16. Strategy, Statecraft, Technology (Changing Character of War) Centre, Oxford University
17. The Hague Centre for Strategic Studies
18. Universidade de Lisboa
19. University of Glasgow
20. Stellenbosch University

International Organizations

21. Center for Civilians in Conflict (CIVIC)
22. Europol
23. International Committee of the Red Cross
24. United Nations Office for the Coordination of Humanitarian Affairs (UN-OCHA)

Private sector

25. BwConsulting. Inhouse Consultancy of the German Armed Forces
26. ESS Maritime
27. IBEX Strategic Solutions
28. Integrated Intelligence, Defence and Security Solutions (I2DS2)
29. PwC Strategy& GmbH
30. Traversals Analytics and Intelligence GmbH

Governmental organization

31. Federal Office of Civil Protection and Disaster Assistance (BBK), Germany
32. Ministry of Defence, Embassy of the Kingdom of the Netherlands

Military Organizations

33. 353rd Civil Affairs Command, U.S. Army Reserve
34. Civil-Military Engagement Group (BEL)
35. Crisis Management and Disaster Response Centre of Excellence
36. DEU MN CIMIC Cmd
37. DtA DEU-NLD Corps G9 Civil Military Cooperation
38. EUCOM J9
39. FINCENT
40. General Command of the Polish Armed Forces
41. HDF Cyber and Information Operations Centre
42. Hellenic National Defense General Staff
43. Homeland Defence Command (Bundeswehr)
44. Irish Defence Forces, Army
45. Latvia NAF JHQ J-9
46. Military Training Centre For Foreign Operations, Poland
47. Multinational CIMIC Group
48. NATO Allied Command Transformation
49. NATO Force Integration Unit Lithuania
50. NATO JFC Brunssum - J9 CIMIC Branch
51. NATO JFC Naples
52. NATO Joint Force Training Centre
53. NATO Space Centre of Excellence
54. NFIU Hungary
55. NLD MOD - Joint Center of Expertise Communication & Engagement
56. Outreach Group, 11 Brigade, British Army
57. Singapore Armed Forces
58. The MoD of the Republic of Slovenia
59. US Marine Corps Civil Military Operations School
60. US Special Operations Command Europe (SOCEUR)
61. Joint Operational HQ - Italy

Address:
Brasserskade 227A
2497 NX The Hague
The Netherlands

Contact Information:
Registry CCOE: +31 (0)889566439
Public Affairs Office: +31 (0)889 566441
E-Mail: info@cimic-coe.org
Webpage: www.cimic-coe.org