CCOEs x

aca CIMICs

-VOL.II-

Module 1: Intro acaCIMICs

acaCIMICs is not a conference - it is a living system. A platform designed to capture, connect, and evolve knowledge at the intersection of academia, industry, and military practice. In an era defined by complexity, hybrid threats, and rapid technological change, no single domain holds all the answers. The future of CIMIC depends on our ability to integrate perspectives, challenge assumptions, and transform knowledge into actionable insight.

The vision of acaCIMICs is to establish a persistent, adaptive knowledge ecosystem - one that bridges operational realities with academic depth, and transforms dialogue into capability. It is built on the understanding that innovation emerges not in isolation, but through structured collaboration across disciplines, sectors, and communities.

At its core, the mission of acaCIMICs is clear:
"To identify, connect, and activate intellectual and operational assets, and to transform their contributions into captured intelligence that strengthens CIMIC across all phases of engagement."

Through this mission, acaCIMICs directly supports the broader objectives of the CCOE's Academic Network in enhancing interoperability, enabling informed decision-making, and fostering a holistic approach aligned with NATO's Comprehensive Approach. By integrating cultural, societal, economic, and military perspectives, the platform contributes to a more resilient and adaptive understanding of modern security challenges.

Module 2: Next Level
(transition from last year to this iteration)

acaCIMICs Volume I: Experimentation – Innovation for a Collaborative Future marked the initial step in operationalising this vision.

The first iteration established acaCIMICs as a dedicated platform where academic, industry, military, and innovation communities could converge. Its focus was on exploring how academic methodologies and experimental approaches could be integrated into CIMIC processes. More than a forum for discussion, Volume I functioned as a testing ground, bringing together diverse assets to co-create analytical tools, challenge established practices, and introduce new ways of thinking.

Through this process, valuable captured intelligence emerged: insights into how collaboration can enhance experimentation, how academic rigor can strengthen operational processes, and how interdisciplinary engagement can unlock new pathways for innovation. Volume I laid the foundation for a growing network of engaged contributors and demonstrated the potential of structured collaboration as a force multiplier.

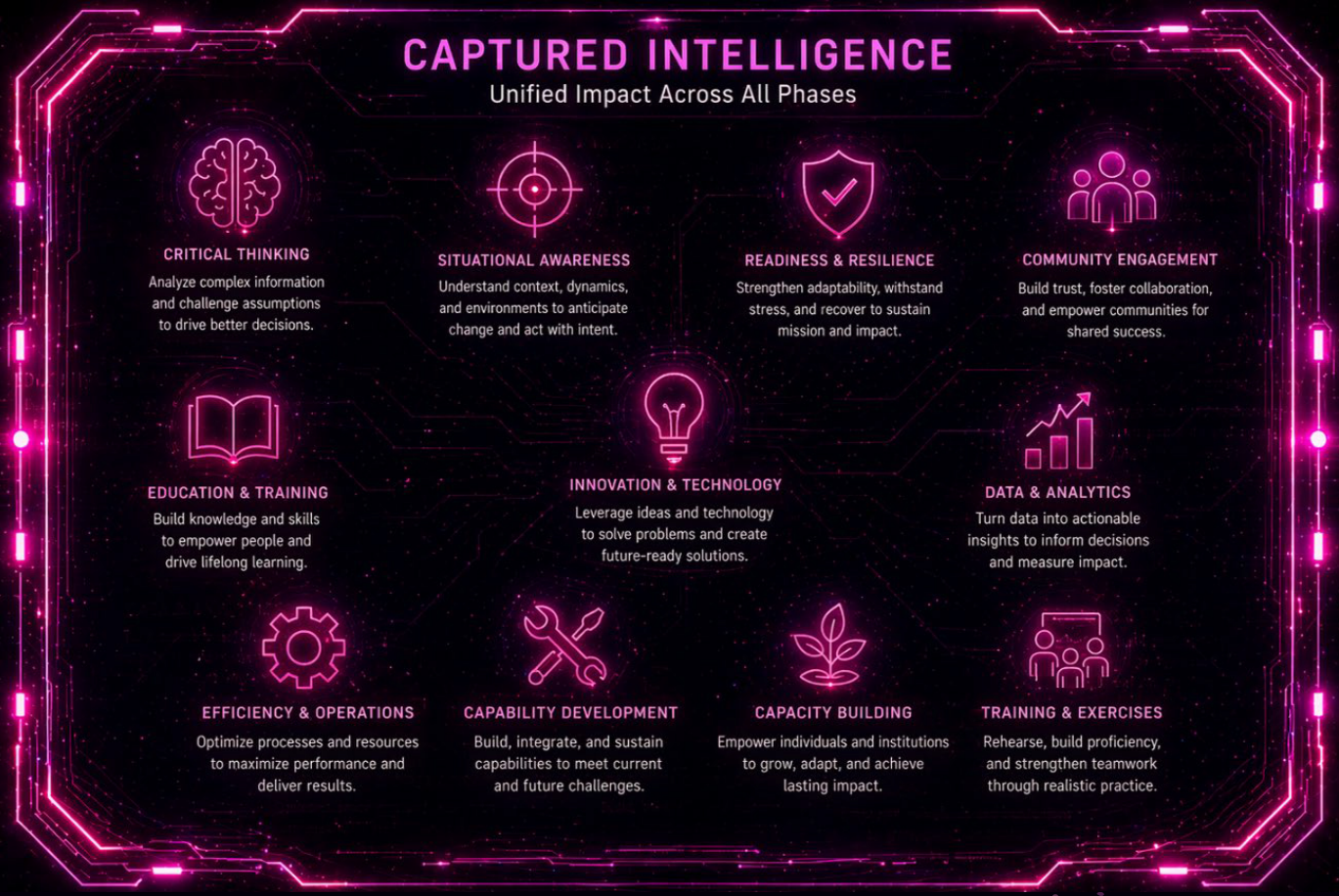
Building on this foundation, acaCIMICs Volume II advances from experimentation to integration.

This iteration focused on consolidating the network, deepening collaboration, and translating ideas into actionable outcomes. The platform brought together a diverse set of assets: military practitioners, academic researchers, and industry experts - each contributing their expertise to a shared objective: enhancing future readiness through collaboration.

Within this volume, these contributions are not presented as isolated inputs, but as captured intelligence; structured, contextualised, and connected. Together, they form a knowledge base that reflects the collective thinking of the acaCIMICs community and provides a foundation for continued development.

Volume II reinforces acaCIMICs as more than an event. It is a system for continuous exchange, a network of expertise, and a mechanism for transforming knowledge into capability. By connecting assets and capturing intelligence, acaCIMICs contributes to a more agile, informed, and resilient approach to CIMIC - ready to meet the challenges of today and anticipate those of tomorrow.

Module 3: acaCIMICs assets



Asset #1: Policy lessons for Domestic CIMIC/Host Nation Capabilities

JAKUB JANDA
Director
European Values Center
for Security Policy (EVC)
jakub.janda@europeanvalues.cz

This contribution showed the results of a series of tabletop exercises conducted in 2025 by the European Values Centre for Security Policy and the Centre for an Informed Society, focusing on a crisis scenario on NATO's Eastern Flank with direct implications for the Czech Republic. The simulations explored what would happen if Russian aggression escalated significantly, placing the Czech Republic in the role of a key transit and support hub. Within a short period, the country would need to manage the arrival of up to 500,000 refugees while simultaneously facilitating the movement of 100,000–150,000 allied troops and heavy equipment.

What became clear through this contribution is how quickly such a situation would overwhelm not just military structures, but the entire civilian system. The scenario showed that cyberattacks on hospitals, energy networks, and transport infrastructure would disrupt essential services almost immediately.

At the same time, disinformation campaigns would fuel panic among the population, leading to bank runs, panic buying, and a loss of confidence in public institutions. These effects would reinforce each other, creating a cascading crisis in which workforce shortages, supply chain disruptions, and social unrest further weaken the state's ability to respond.

The contribution also highlighted that the main challenge is not a lack of individual capabilities, but a lack of coordination between them. Government bodies, regional authorities, the military, businesses, and NGOs all play important roles, yet their planning and response mechanisms remain fragmented. Weak strategic communication makes it difficult to counter disinformation effectively, while limited capacity in healthcare and social services reduces the system's ability to absorb shocks. Businesses and civil society actors, despite their potential, are not sufficiently integrated into crisis planning.

At the same time, the exercises pointed toward practical ways to strengthen resilience. They showed the importance of building integrated planning structures that connect all relevant actors before a crisis occurs. Improving cyber resilience, strengthening public communication, and involving businesses more actively in preparedness, through stress testing, workforce planning, and crisis communication, were identified as key steps. The contribution also emphasised the role of communities, suggesting the use of volunteer networks and diaspora engagement, as well as the need to better equip regional authorities with resources and planning capacities.

Overall, this contribution showed that in a modern crisis, military effectiveness depends heavily on the stability and resilience of civilian systems. Supporting troop movements, maintaining public order, and ensuring economic continuity are all interconnected tasks that require close cooperation between civilian and military actors.

This directly connects to CIMIC, as it highlights the need for a permanent and well-integrated framework that links military requirements with civilian capabilities. CIMIC is not just about coordination during operations, but about building relationships, structures, and trust in advance so that cooperation works under pressure. In light of the

Asset #2: Autonomous Drone Detection, Identification & Tracking via No-Code Computer Vision AI Platform

DR. TARIK HUBANA
Chief Operating Officer,
EU Operations
www.artianalytics.com

This contribution showed how emerging technologies, specifically no-code artificial intelligence, can transform the way military and civilian actors approach situational awareness and threat detection in complex operational environments. Focusing on a case study presented by ARTI Analytics, it demonstrated the development and deployment of an autonomous drone detection, identification, and tracking system built entirely through a no-code computer vision platform.

What this contribution made particularly clear is that the growing reliance on aerial monitoring and early-warning systems is increasingly constrained not by technology itself, but by access to expertise and secure infrastructure. Unauthorised drones pose a direct threat to critical infrastructure, logistics, and operational security, yet many units lack the in-house capacity to develop and deploy real-time detection systems. At the same time, strict security requirements prevent sensitive operational data from being processed in external or cloud-based environments. The contribution showed that this combination of technical complexity and security constraints creates a significant capability gap across both military and civilian organisations.

Against this backdrop, the case study demonstrated how a no-code AI platform can bridge this gap by enabling non-specialists to build, train, and deploy computer vision models using their own data, entirely within secure, on-premises systems. Through guided workflows, including data ingestion, automated model optimisation, and deployment, users are able to generate operational detection capabilities without writing code or relying on external AI experts. This approach not only simplifies the technical barrier, but also ensures that sensitive data, including video streams and model outputs, remain within classified environments at all times. The contribution further showed that this approach has immediate operational benefits. Experimental results highlighted a significant reduction in deployment time for detection systems, increased self-sufficiency among units, and stronger data security through fully controlled processing pipelines. In practical terms, this means that both military and civil protection actors can rapidly establish automated perimeter monitoring, detect and classify aerial threats in real time, and respond more quickly to emerging risks. The system's ability to integrate real-time sensor data and provide early warning enhances situational awareness in a way that is both scalable and adaptable to different operational contexts.

Importantly, the contribution also illustrated a broader shift in how technological capabilities are distributed. Rather than relying on centralised expertise or external providers, capabilities can be generated at the operational level, directly by the actors who need them. This "democratisation" of AI not only accelerates response times but also reduces dependency on external support, which is particularly critical in crisis or contested environments.

At the same time, the emphasis on secure, on-premises deployment ensures that these capabilities remain compatible with strict military and governmental security requirements.

Technological innovation can significantly strengthen preparedness and responsiveness in civil-military contexts, but only when it is designed to be usable, secure, and directly relevant to operational needs. The real challenge is not access to advanced tools, but ensuring that they can be applied effectively by a wide range of actors working under practical constraints and time pressure.

In a CIMIC context, this becomes particularly important, as effective cooperation depends on shared understanding and compatible capabilities across military and civilian stakeholders. Building and maintaining a common operational picture, along with the ability to generate and exchange actionable information in real time, is increasingly central to success. Technologies such as no-code AI platforms support this by enabling different actors to contribute to situational awareness while keeping sensitive data within secure boundaries. At the same time, their decentralised use introduces new risks of fragmentation if systems are developed and applied independently. This raises a critical question: if such tools allow capabilities to emerge at the operational level across multiple actors, how can CIMIC structures ensure that they remain interoperable, coordinated, and aligned with broader mission objectives in a complex, multi-actor environment?

Asset #3: Immersive VR for CIMIC – Advancing Education Through Simulation

DR. VLAD NICULESCU DINCA
Assistant Professor
Institute for Security and Global Affairs
https://www.universiteitleiden.nl/en/staffmembers/vlad-niculescu-dinca
ERIK JAN BIJVANK
CDO, Scopic Labs VR Studio
www.scopiclabs.com

This contribution showed how immersive virtual reality (VR) can reshape the training of CIMIC personnel by bringing them closer to the realities of complex operational environments. It started from the observation that CIMIC does not operate in controlled or predictable settings, but in situations marked by uncertainty, time pressure, and interactions between diverse actors with competing interests. Traditional training methods, while still valuable, are limited in their ability to replicate these dynamics, often simplifying scenarios and reducing the emotional and cognitive pressures that define real-world operations.

What the contribution made clear is that this gap in training directly affects the development of key CIMIC competencies. Skills such as negotiation, communication, situational awareness, and interagency coordination are inherently relational and context-dependent. They cannot be fully developed through static case studies or classroom-based instruction alone. Instead, they require exposure to evolving situations where decisions must be made with incomplete information and where actions have visible consequences.

In this context, VR was presented as a way to bridge the gap between theory and practice. By creating immersive and interactive environments, VR allows participants to experience complex scenarios rather than simply learn about them. The contribution illustrated this through the example of a simulated fragile urban setting, where military personnel must engage with local authorities, NGOs, and other stakeholders. Within such environments, participants can practise communication under pressure, manage misunderstandings, and navigate competing priorities, all while observing how their decisions shape the unfolding situation.

A central strength of the approach lies in its structured alignment between CIMIC competencies and VR applications. Rather than treating VR as a general training tool, the contribution showed how it can be purposefully linked to specific skill areas. Strategic communication can be trained through multi-actor dialogue simulations, situational analysis through dynamic scenarios that reveal cause-and-effect relationships, and interagency collaboration through shared virtual environments that require coordination and trustbuilding. This targeted use ensures that the technology directly supports professional requirements, rather than adding complexity without clear benefit.

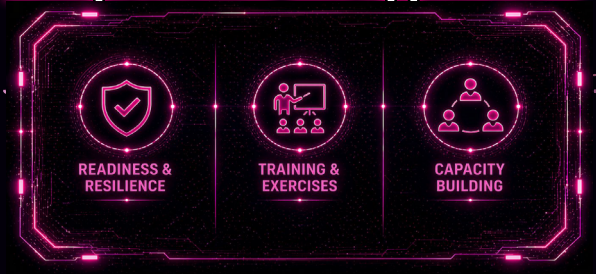
Another important aspect highlighted was the psychological realism of VR. Because participants experience a strong sense of presence, they react not only cognitively but also emotionally. This enables the development of skills that are difficult to train otherwise, such as managing stress, exercising empathy, and making decisions under pressure. In this sense, VR contributes to building reflective practitioners who are better prepared to handle the human dimension of CIMIC operations.

At the same time, the contribution emphasised that VR should not be seen as a replacement for existing training methods, but as a complement to them. Its effectiveness depends on how well it is integrated into broader learning frameworks, including clear objectives, guided reflection, and structured debriefing. It also acknowledged the need for further research on how such technologies influence learning outcomes over time and how they can be scaled effectively across institutions.

Overall, this contribution showed that preparing CIMIC personnel for modern operations requires training approaches that genuinely reflect the complexity and human dynamics of real-world environments. VR offers a practical way to do this by creating controlled yet immersive settings in which participants can experience uncertainty, interaction, and pressure first-hand. In doing so, it supports the development not only of technical understanding, but also of the interpersonal and analytical skills that lie at the heart of effective CIMIC.

This naturally ties back to CIMIC's core function: understanding the civil environment and engaging meaningfully with a wide range of actors. If these competencies are best developed through immersive and experiential learning, then VR is not just an additional tool, but a way to strengthen how CIMIC is learned and applied in practice. It shifts training from abstract preparation to shared experience, where coordination and interaction can be developed before they are tested in reality. This raises a critical question: if VR can realistically recreate the complexity of civil-military environments, how can CIMIC institutions ensure that such training is systematically integrated and shared across both military and civilian actors, so that coordination in real operations is built in advance rather than improvised under pressure?

Asset #4: NATO CIMIC in a Domestic Context: Comparing National Interpretations and Applications



SONJA GRUENBAUER
Consultant
Civil-Military Cooperation
Centre of Excellence
Sonja.gruenbauer@gmx.de

This contribution showed how the concept of CIMIC, while well established within NATO doctrine, becomes significantly more complex and ambiguous when applied in domestic contexts. It began by situating CIMIC within today's security environment, characterised by persistent competition, hybrid threats, and the increasing likelihood that future crises (especially under Article 5) will unfold within Allied territory rather than abroad. In this setting, resilience is no longer a supporting concept but a central pillar of deterrence and defence, requiring effective cooperation between military forces and civilian authorities across multiple domains.

What the contribution made particularly clear is that CIMIC was primarily designed for expeditionary operations, and its transfer into domestic environments introduces uncertainty about its role and function. This is reflected in a core issue of conceptual ambiguity: CIMIC is interpreted differently across nations and institutions, sometimes as a joint military function and at other times as a supporting activity.

Such inconsistencies affect how it is integrated and applied, creating friction between civilian and military stakeholders in situations where alignment is critical.

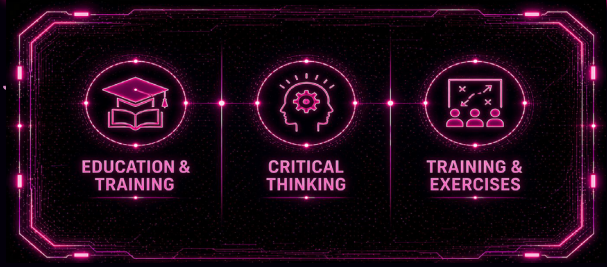
To explore this, the research adopted a comparative case study approach, focusing on Germany, Spain, and Finland. These cases represent different legal frameworks, security cultures, and models of civil preparedness, ranging from more restrictive approaches to comprehensive whole-of-society defence concepts. By assessing these national practices against NATO CIMIC doctrine, the contribution identified both areas of alignment and key divergences, particularly in command structures, civil-military interfaces, and perceptions of legitimacy and trust.

A central insight is that the challenges are not only operational but structural. Institutional fragmentation, differing legal authorities, and varying levels of trust all shape how CIMIC functions in domestic contexts. In addition, gaps in training and inconsistent doctrinal interpretations make it difficult to establish a shared understanding across actors. These issues become especially critical in multi-domain scenarios, where military support to civil authorities must be delivered quickly, coherently, and in a way that maintains public legitimacy.

The contribution therefore pointed toward the need for greater conceptual clarity and stronger alignment between NATO frameworks and national practices. This includes clearer definitions of CIMIC roles in domestic settings, improved institutional integration, and more consistent training and exercise structures involving both civilian and military stakeholders.

Taken together, this shows that as the focus of operations shifts toward domestic and multidomain environments, CIMIC must evolve from an ambiguously applied concept into a clearly defined and integrated function within national and NATO defence systems. If this does not happen, existing coordination gaps risk becoming a decisive weakness in crisis situations, raising the critical question of how a shared and operationally coherent understanding of CIMIC can be established in advance, rather than tested for the first time under the pressure of a real-world emergency.

Asset #5: Enhancing Student Engagement and Learning through Game-Based Learning with PeaceMaker



MARNO SWART
Lecturer at the Department of Political Science, Faculty of Military Science
Stellenbosch University
marnoswart@sun.ac.za

This contribution explored how game-based learning can be used to improve the teaching of complex concepts in international relations and civil-military relations, using the simulation game ***PeaceMaker*** as a central example. It was grounded in a practical teaching context at Stellenbosch University, where consistently low pass rates - averaging around 37% between 2004 and 2021 - highlighted the limitations of traditional, lecture-based approaches in helping students engage with abstract theory.

In response, the contribution showed how integrating interactive and visual learning methods can create a more engaging and effective learning environment. Instead of relying solely on lectures, the approach combined theoretical instruction with simulation-based exercises. Students were first introduced to key concepts and then applied them in the PeaceMaker simulation, taking on leadership roles and making decisions in a dynamic political environment shaped by real-world constraints. This shifted learning from passive absorption to active engagement, where theory became something to test, experience, and reflect upon.

A key insight was that the value of the simulation did not lie in the technology itself, but in how it was embedded within the teaching process. The structured cycle, moving from theory to simulation and back to guided reflection, allowed students to engage more deeply with the material and helped identify where misunderstandings occurred. It also reinforced the importance of combining different forms of learning, particularly visual and interactive elements, which can strengthen both comprehension and retention.

The results of this shift were significant. Following the introduction of game-based learning, pass rates increased markedly, reaching over 80% in 2023 before stabilising at a higher level than in previous years. More importantly, students became more actively involved in the learning process and showed a stronger ability to engage with key concepts, such as the roles of international actors and the challenges of decision-making under pressure.

At the same time, the contribution highlighted an important limitation. While engagement improved, many students still struggled to apply theoretical frameworks in a deeper and more critical way. This pointed to the need for additional measures to explicitly connect theory and practice and to strengthen analytical thinking beyond the simulation itself.

Seen through a CIMIC lens, this contribution underlines how essential it is to move beyond purely theoretical instruction and towards learning approaches that reflect the complexity of real-world interaction.

CIMIC requires practitioners who can interpret situations, balance competing interests, and make informed decisions in dynamic environments; skills that are difficult to develop without some form of experiential learning. At the same time, the experience here suggests that engagement alone is not enough; it must be paired with structured reflection and a solid grounding in theory. This raises an important consideration: if immersive and game-based approaches make learning more accessible and engaging, how can CIMIC training ensure that this engagement translates into deeper analytical thinking and not just more intuitive, but potentially unexamined, decision-making in real operations?

Asset #6: Civil-Military Cooperation: Working together in a new geopolitical reality

CELESTINE DE ZEEUW
Researcher
TNO Defense and Security
celestine.dezeeuw@tno.nl

This contribution examined how CIMIC is evolving in response to a fundamentally changing security environment, using the work of TNO as a starting point. It highlighted a clear shift in focus: from expeditionary missions and support to civil authorities toward the defence of national and allied territory. In this new context, crises are no longer distant or contained; they unfold within domestic space, across interconnected domains, and often in the grey zone between peace and conflict.

What emerged strongly from the contribution is that this shift changes the nature of civil-military interaction. Where earlier models often assumed a supporting role for the military or a clearly defined division of responsibilities, current and future scenarios require a much deeper level of integration. Military operations are increasingly dependent on civilian systems (transport networks, energy infrastructure, data systems, healthcare), and broader societal resilience. As a result, civil and military actors can no longer operate in parallel; they must function as part of a single, interconnected ecosystem.

At the same time, the contribution showed that the conceptual and practical foundations for this level of cooperation are still underdeveloped. A key challenge lies in the diversity of perspectives and definitions surrounding CIMIC. The distinction between traditional CIMIC, anchored in military doctrine, and broader forms of civil-military collaboration creates ambiguity in roles, expectations, and governance structures. This makes coordination more complex, particularly in high-pressure situations where clarity and speed are essential.

To address this complexity, the contribution introduced the idea of treating cooperation itself as something that can be deliberately designed rather than assumed. Using a "morphological design" approach, it proposed breaking down cooperation into key variables, such as actor composition, governance structures, legal frameworks, levels of trust, and information-sharing practices. By making these dimensions explicit, practitioners can better understand the "DNA" of a given cooperation setup, anticipate challenges, and align expectations before crises occur. This perspective shifts the focus from reacting to crises toward actively shaping the conditions for effective collaboration. It emphasises that each form of cooperation comes with its own dynamics, risks, and requirements, and that these need to be understood and discussed in advance. Without this shared understanding, even well-intentioned cooperation can break down when confronted with uncertainty, time pressure, or conflicting assumptions.

From a CIMIC standpoint, this contribution highlights a broader transformation in how civil military interaction is understood and practiced. As dependence on civilian systems increases, cooperation can no longer be treated as a supporting activity that is activated when needed, but must be considered a continuous and structured element of preparedness. This shifts attention toward how relationships are built, how responsibilities

are perceived, and how information is shared across different actors over time. It also suggests that effectiveness in crisis situations is shaped long before a crisis begins, through how well these underlying dynamics are understood and aligned. This leads to a different but equally important question: if CIMIC now spans a wide range of actors, contexts, and phases of conflict, how can its structures remain flexible enough to adapt to different forms of cooperation while still providing enough clarity to guide action in fast-moving and uncertain situations?

Asset #7: Strengthening civilian, government and military partnerships in support of conflict preparedness in Europe

RORY MOYLAN
Head of Region MENA and Europe
British Red Cross
rorymoylan@redcross.org.uk
CLAIRE CLEMENT
Director of International Law and Policy
British Red Cross
claireclement@redcross.org.uk

This contribution examined how preparedness is being approached in practice across Europe, with a particular focus on strengthening cooperation between civilian actors, governments, and the military. Drawing on the work of the British Red Cross, it highlighted a rapidly evolving security environment shaped by hybrid threats, the increasing risk of large-scale conflict, climate impacts, and broader systemic shocks. In this context, preparedness is no longer a sector-specific responsibility, but a shared challenge that requires coordinated action across society.

A central point of the contribution is that, despite growing awareness, preparedness efforts across Europe remain uneven and often fragmented. While concepts such as "whole-ofsociety" resilience are widely recognised, their implementation is still inconsistent, with significant gaps in population preparedness and varying levels of integration between civil, military, and private-sector actors. CIMIC has improved in some areas, but it remains far from uniformly embedded, and coordination mechanisms are often underdeveloped or insufficiently tested.

The contribution also highlighted the unique role of National Red Cross and Red Crescent Societies as bridging actors. Positioned between communities, governments, and humanitarian systems, they are able to connect different layers of society and facilitate cooperation in times of crisis. In this role, they contribute not only to response efforts but also to preparedness by supporting coordination, building trust, and strengthening links between formal institutions and local communities.

One of the key practical insights presented was the role of Memoranda of Understanding (MOUs) between governments and National Societies. These agreements were shown to be effective tools for clarifying roles and responsibilities, particularly in situations where legal frameworks are unclear or outdated. They can also help define civil-military coordination mechanisms, align planning and training efforts, and create a shared understanding of how different actors should operate in crisis situations. At the same time, MOUs serve as instruments of humanitarian diplomacy, helping to safeguard the space for principled humanitarian action while enabling cooperation with military and governmental actors.

The contribution further emphasised the importance of moving from policy discussions to practical implementation. Initiatives such as international conferences, roundtables, and jointexercises were presented as ways to strengthen coordination, share lessons learned, and test preparedness frameworks under realistic conditions. Particular attention was given to the need for a "twin-track" approach, combining efforts to improve population-level preparedness, through education, volunteering, and community engagement, with efforts to enhance civil-military coordination and interoperability.

At its core, this contribution showed that preparedness depends not only on formal structures, but on how well different actors are connected, aligned, and able to act together under pressure. Gaps in coordination, unclear roles, and limited engagement with communities can undermine even well-developed plans, while strong partnerships and shared understanding can significantly enhance resilience.

In a CIMIC context, this reinforces the importance of building relationships that extend beyond institutional boundaries and include civil society as an active partner. Effective cooperation is not only about aligning military and governmental actors, but also about integrating community-level perspectives and capacities into preparedness efforts. This points to a broader challenge: if whole-of-society preparedness is to become a reality rather than an aspiration, how can CIMIC structures ensure that civil society actors, particularly those embedded in communities, are meaningfully integrated into planning, coordination, and decision-making processes without compromising their independence and humanitarian principles?

Asset #8: CMCC: Redefining Civil-Military Synergies in Gaza and Beyond

ELENA URSU
World Food Program
elena.ursu@wfp.org

This contribution examined the establishment and functioning of the Civil-Military Coordination Centre (CMCC) as a practical response to one of the most complex and sensitive operational environments. Created in October 2025, the CMCC was designed as a structured platform to facilitate interaction between military, diplomatic, and humanitarian actors in support of ceasefire arrangements and the delivery of assistance. Rather than acting as a command structure, it serves as a convening space where different stakeholders can exchange information, raise concerns, and work through operational challenges within their respective mandates.

A central theme throughout the contribution is the need for structured dialogue in highly fragmented and politically charged environments. In situations where multiple actors operate under different mandates and principles, the absence of coordination can quickly lead to misunderstandings, duplication of efforts, or blocked access for humanitarian operations. The CMCC addresses this by providing a regular forum for engagement, helping to create a shared understanding of constraints and priorities while maintaining the independence of each actor involved.

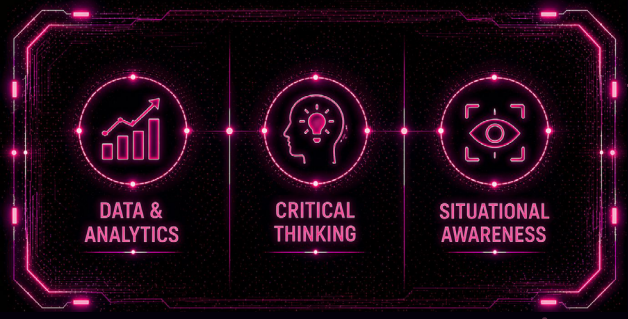
In practice, the CMCC operates through a combination of plenary sessions, thematic working groups, and regular briefings. These formats allow participants to move beyond general updates and focus on specific issues such as medical evacuations, access routes, or the handling of sensitive materials. By consolidating fragmented information into a more coherent picture, the platform supports more informed decision-making, even though authority remains with the individual organisations. This approach helps to make coordination more predictable and transparent in an otherwise volatile environment.

Another important aspect highlighted in the contribution is the CMCC's ability to adapt over time. Its structure and working methods have evolved in response to operational needs, shifting from more rigid formats to flexible, theme-based discussions that better reflect realities on the ground. This continuous adjustment has been essential in maintaining relevance, especially as the context has moved from immediate ceasefire implementation toward broader questions of aid quality, access, and longer-term stabilisation.

At the same time, the contribution underscored the sensitivities inherent in civil-military coordination in such contexts. Maintaining clear boundaries between coordination and command, and safeguarding humanitarian principles such as neutrality and independence, remain critical. The potential introduction of additional actors, such as an international security force, could further complicate these dynamics by blurring lines between security and humanitarian roles. In this respect, the CMCC not only facilitates coordination but also acts as a space where these tensions must be continuously managed and negotiated.

Viewed through a CIMIC lens, this contribution highlights the practical realities of coordination in high-intensity, politically sensitive environments, where cooperation cannot be taken for granted but must be actively maintained. It shows that effective civil-military interaction depends less on formal structures alone and more on the ability to create spaces for dialogue, build mutual understanding, and adapt to changing conditions while respecting different mandates. This brings forward a more practical but still critical question: when time pressure, security constraints, and competing priorities intensify, how can CIMIC practitioners ensure that coordination platforms like the CMCC actually lead to timely, actionable decisions on the ground rather than becoming forums for discussion without operational impact?

Asset #9: Making Sense of Complexity & Humanitarian Analysis in Practice



LARS PETER NISSEN
CEO
ACAPS
lpn@acaps.org

This contribution focused on how analysis is conducted in crisis and humanitarian contexts, challenging conventional assumptions about data, decision-making, and objectivity. Drawing on the ACAPS analytical approach, it emphasised that analysis is not simply about collecting more information, but about making sense of incomplete, ambiguous, and often contradictory data under pressure.

At the heart of the presentation was the recognition that analysts rarely operate under ideal conditions. Instead, they face four persistent constraints: ambiguity, uncertainty, limited time, and restricted capacity to process information. These factors shape not only what can be known, but also how decisions are made. In such environments, waiting for complete or perfect data is not an option, and the focus must shift toward producing insights that are useful and timely, even if they remain imperfect.

To address this, the contribution introduced three guiding principles: understanding what information is actually needed, prioritising sense-making over raw data accumulation, and accepting that being approximately right is often more valuable than being precisely wrong. This reframing highlights the importance of judgement, prioritisation, and clarity in analysis, particularly when decisions must be taken quickly and with real-world consequences.

A significant part of the contribution also explored how human biases influence analytical processes. Through practical examples and exercises, it showed how easily individuals fall into patterns such as confirming their own assumptions, stopping the search for alternatives too early, or relying on incomplete information to draw conclusions. These biases are particularlydifficult to detect because they feel correct in the moment, making them a persistent and often invisible challenge in analytical work.

Another key insight was the role of narratives in shaping how information is interpreted and communicated. The way data is framed can strongly influence understanding, sometimes highlighting certain aspects while obscuring others. This underscores the need for analysts to remain aware not only of the data they use, but also of the assumptions and stories that guide their interpretation.

Taken together, this contribution showed that effective analysis in crisis settings is less about precision and more about navigating uncertainty in a structured and reflective way. It requires constant awareness of limitations, both in the available data and in one's own thinking, and a willingness to question initial assumptions rather than reinforce them.

In a CIMIC context, this has direct implications for how information is shared, interpreted, and used across military and civilian actors. Coordination often depends on a shared understanding of complex and evolving situations, yet this understanding is shaped by different perspectives, mandates, and analytical approaches. Recognising the limits of data and the influence of bias becomes essential for building a more reliable common operational picture. This leads to a practical and critical question: when multiple actors bring their own assumptions, time pressures, and partial information into a shared decision-making process, how can CIMIC practitioners ensure that analysis is continuously questioned and refined rather than prematurely accepted as a stable basis for action?

Asset #10: Building Societal Resilience Through CIMIC Experimentation: A Framework for Eastern Flank Civil-Military Exercises

ANDREI OCNEANU
cimic staff officer
headquarters multinational division south-east, romanian ministry of defense
andrei.ocneanu88@gmail.com

This contribution focused on how societal resilience can be strengthened through more structured and realistic civil-military exercises, particularly on NATO's Eastern Flank. It was grounded in both operational experience and recent developments in the security environment, where the threat of large-scale conflict has shifted attention toward preparedness within Allied territory. In this context, resilience is no longer seen as a supporting factor, but as an operational condition that directly influences deterrence and defence.

A key starting point of the contribution was the observation that current approaches to CIMIC exercises often fall short of this requirement. While many exercises include civil components, they tend to remain fragmented, with limited integration at the operational level. Civil analysis is frequently inconsistent, data is not systematically used, and insights generated during exercises rarely translate into concrete decision-making. As a result, valuable information is collected, but not effectively turned into operational impact.

Drawing on practical examples, from CIMIC Victory in Romania to experiences at HQ MND-SE and KFOR, the contribution highlighted recurring patterns. Access to civilian actors and environments can be achieved, and initial cooperation can be established, but these efforts often lack continuity, structure, and mechanisms for sustained integration. Coordination tends to rely on ad hoc arrangements, and while trust can be built, it is not always embedded in a lasting framework. This creates a gap between short-term engagement and long-term resilience building.

To address this, the contribution proposed the development of a structured exercise framework for the Eastern Flank, designed to better integrate civil and military elements across different levels. The idea is to move beyond isolated exercises toward a continuous, repeatable model that links local actors, national institutions, and NATO structures. By doing so, exercises could generate comparable data, strengthen interoperability, and provide actionable insights for both operational and strategic levels. Importantly, such a framework would not only test military capabilities but also examine how civilian systems and communities respond under stress.

Underlying this proposal is a broader shift in thinking: resilience is built from the bottom up, through communities and local actors, but it must be coordinated from the top down to be effective. Civil preparedness, therefore, becomes the space where these layers meet inpractice. Exercises that bring together military units, civil authorities, and society at large can help bridge this gap, but only if they are designed to capture, analyse, and apply lessons in a structured way.

In a CIMIC context, this contribution reinforces the idea that cooperation must go beyond participation in exercises and evolve into a sustained process of integration, learning, and adaptation. If resilience is to function as a deterrent, then civil-military interaction must be continuously tested, refined, and embedded into planning and decision-making processes. This points to a practical challenge for CIMIC: if exercises are meant to generate real operational value, how can their outcomes be systematically captured, translated, and fed back into both military and civilian decision-making cycles, rather than remaining isolated lessons learned?

Asset #11: TDF CIMIC Integration in local crisis preparedness and management

WOJCIECH KAZANECKI, PhD
Assistant Professor
Institute of Administration and Political Science, University College of Professional Education
wojciech.kazanecki@wskz.pl

This contribution examined how CIMIC is developing within Poland's Territorial Defence Forces (TDF), particularly in response to a changing threat landscape that combines hybrid warfare and natural disasters. It highlighted that local-level crises, ranging from flooding and infrastructure disruptions to disinformation campaigns, are increasingly interconnected, directly affecting societal stability and requiring coordinated responses between military units, local authorities, and communities.

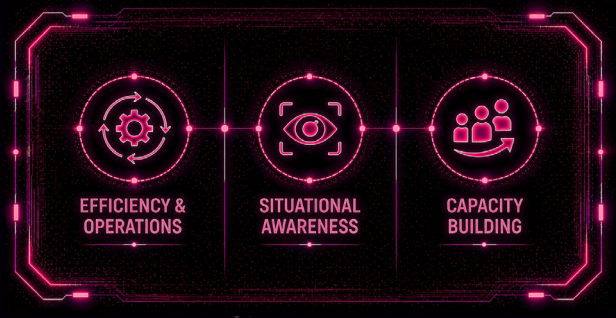
A central theme of the contribution is the growing importance of societal resilience as a form of defence. Hybrid threats, such as disinformation and efforts to deepen political polarisation, aim to weaken trust in institutions and reduce collective cohesion. In this context,strengthening the relationship between the military and society becomes a key element of deterrence, as public trust and engagement can influence how effectively a society responds to both external and internal pressures.

The contribution showed that the TDF is actively working to build these connections, particularly through cooperation with local administrations and involvement in crisis response activities. There is evidence of gradual improvement in crisis management procedures and coordination, as well as increasing efforts to embed the military more closely within local communities. However, this process is still evolving and faces several challenges, including differences in roles and expectations between various military branches and the need to align military activities with civilian structures and priorities.

One of the more practical insights concerns the use of After Action Reviews (AARs) at the local level. While there have been some attempts to introduce this approach, its application remains limited and often ad hoc. This reflects a broader difficulty in turning operational experience into structured learning that can guide future action. At the same time, the contribution highlighted the importance of communication and transparency in strengthening civil-military relations, as well as the need for continued engagement through joint exercises and visible presence within communities.

In a CIMIC context, this contribution underscores the importance of building resilience through sustained, locally grounded cooperation. It shows that effectiveness depends not only on formal structures, but also on how well relationships, communication, and shared understanding are developed over time. This leads to a critical question that sits at the heart of this case: if Territorial Defence Forces are meant to act as a bridge between the military and local society, how can they clearly define and communicate their role in a way that strengthens trust and avoids confusion or overlap with other military and civilian actors in times of crisis?

Asset #12: Situational CIMIC Design: A Situational Approach to Civil–Military Interaction during Execution



KLAS LINDSTRÖM
SWEDISH ARMED FORCES
Joint Forces Command
Klas.Lindstrom@4cstrategies.com

This contribution explored a practical challenge at the core of modern civil-military interaction: how to act together effectively during ongoing operations when full alignment between civilian and military actors is not yet in place. Drawing on a Swedish total defence context, it highlighted that while doctrine, planning, and coordination structures are well developed, they do not fully resolve the realities of execution under time pressure, uncertainty, and rapidly changing conditions.

A key insight is that the main gap is not conceptual, but practical. Civilian and military actors often enter operations with different mandates, priorities, and decision-making logics. These differences are not flaws, but necessary features of their respective roles. However, when operations accelerate and situations evolve faster than coordination can keep up, these differences can create friction that slows down action or reduces effectiveness. In such moments, waiting for full alignment is not an option, yet acting without coordination risks unintended consequences.

To address this, the contribution proposed a shift in focus, from broad coordination principles to a limited set of recurring "standard situations" where civil-military interaction becomes decisive for operational outcomes. These situations, such as urgent military reliance on civilian infrastructure or sudden operational changes requiring rapid realignment, are not theoretical constructs but patterns repeatedly observed in practice. By narrowing the scope to situations that matter most during execution, the approach makes the problem more concrete and manageable. Each of these situations is paired with a so-called "handrail" - a simple, situationspecific interaction logic designed to guide actors in the first moments of engagement. Rather than providing rigid procedures, these handrails offer a situation-specific interaction logic that helps actors move forward under pressure without prescribing actions. helping actors quickly identify the problem, clarify constraints, and move toward actionable outcomes. The intention is not to replace judgement or existing frameworks, but to provide a shared starting point that reduces hesitation and enables cooperation under pressure.

Initial testing of this approach showed promising results. Even without prior exposure, participants were able to use the handrails to move from fragmented perspectives toward a more shared understanding and coordinated action. What stood out was not the elimination of differences but the ability to work through them more effectively. The approach helped shift focus from positions and assumptions toward operational effects and practical solutions, improving both the speed and quality of interaction.

Looking at CIMIC as military function, this contribution offers a concrete way of addressing one of the field's most persistent challenges: how to enable effective cooperation in real time, when conditions are far from ideal. It suggests that rather than striving for perfect alignment before action, CIMIC may need to focus more on enabling structured interaction during execution itself. This leads to a practical and critical question: if operations increasingly require acting together before full coordination is achieved, how can CIMIC ensure that actors are trained not just to align in advance, but to navigate and manage misalignment effectively while operations are already underway?

Asset #13: A Practical Method for CIMIC operators to counter disinformation in hybrid environments

RICCARDO PASTORE
Independent Researcher
ALICE FELLI
Independent Researcher
BusinessMindsetDeveloper@gmail.com

This contribution addressed a growing operational challenge in modern civil-military environments: how CIMIC practitioners can respond effectively to disinformation and rapidly evolving narratives when decisions must be made before facts are fully verified. It highlighted that in hybrid contexts, civil information is no longer a background factor, but a driver of perception, behaviour, and ultimately operational outcomes. Narratives can spread faster thanverification processes, shaping reactions on the ground and creating immediate risks for freedom of movement, force protection, and legitimacy.

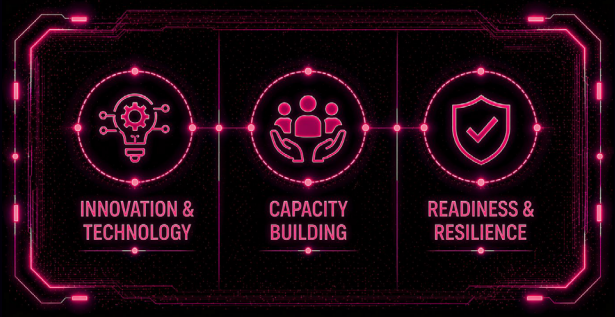
A key insight of the contribution is the existence of a "decision gap." While information flows at high speed through digital and social channels, structured analysis often lags behind. This creates situations where CIMIC actors must act under uncertainty, without clear attribution or confirmed intelligence. The example of the Gossi incident illustrated how quickly a narrative, regardless of its accuracy, can trigger protests, hostility, and operational constraints, forcing decisions to be made under conditions where behavioural effects may emerge before verification is complete. To address this, the contribution introduced the Narrative Risk Appraisal Techniques (NRAT), a simplified and operationally focused structured decisionsupport method. Rather than aiming to determine what is true, NRAT helps structure uncertainty by considering multiple plausible explanations and assessing their potential impact on the civil environment. By shifting the focus from truth to risk, it enables CIMIC practitioners to prioritise early engagement and mitigation measures, even when information remains incomplete.

In practice, this means moving from a reactive approach, waiting for confirmation, to a proactive one that anticipates how narratives may influence behaviour and escalation. The NRAT framework condenses analysis into a rapid cycle: identifying signals, mapping possible explanations, evaluating indicators, projecting civil risks, and informing immediate action. This structured approach allows CIMIC operators to generate decision-relevant insights within a compressed timeframe, supporting engagement with local actors and helping to prevent escalation before it intensifies.

The contribution also emphasised that the challenge is not a lack of information, but a lack of structure in how that information is processed and used. In information-saturated environments, the ability to organise and interpret signals quickly becomes an operational capability in itself. By integrating tools like NRAT into existing CIMIC processes, analysis can become more directly linked to action, supporting both situational awareness and decisionmaking under pressure.

In a CIMIC context, this contribution highlights the increasing importance of understanding and managing the information environment as an integral part of civil-military interaction. It shows that maintaining legitimacy and operational effectiveness depends not only on physical actions, but also on how narratives are perceived and addressed in real time. This brings forward a key dilemma: if CIMIC actors may need to support early and proportionate engagement before verified facts are fully available how can they ensure that early engagement is both timely and measured, without unintentionally amplifying false narratives or contributing to further escalation?

Asset #14: Reimagining Civil-Military Cooperation for future hybrid warfare



ZURAB BEZHANISHVILI
Independent Researcher
zurab.bezhanishvili@yahoo.com

This contribution examined how CIMIC needs to evolve in response to the growing complexity of hybrid warfare and the broader transformation of societies. It started from the observation that emerging threats are no longer confined to traditional military domains, but increasingly target social structures, information environments, and technological systems. Factors such as disinformation, the weaponisation of science, the digital divide, and the erosion of societal cohesion were identified as key challenges shaping the future operating environment.

Building on this, the contribution argued that traditional CIMIC models are no longer sufficient to address these developments. It highlighted how different types of societies, ranging from security-oriented to economically or socially driven systems, shape the way civil-military interaction functions. This diversity means that CIMIC cannot rely on a one-size-fits-all approach, but must adapt to varying societal contexts, governance structures, and expectations. In this sense, CIMIC becomes not just a functional tool, but a reflection of the society in which it operates.

The contribution also traced the evolution of civil defence and CIMIC functions, showing a clear shift from traditional, state-centred approaches toward more comprehensive and integrated models. Modern concepts of total defence increasingly involve civilian actors, volunteers, and private-sector stakeholders, while also addressing hybrid threats that combine physical, digital, and cognitive dimensions. This expansion reflects a broader understanding of security, where resilience depends on the interaction between multiple layers of society.

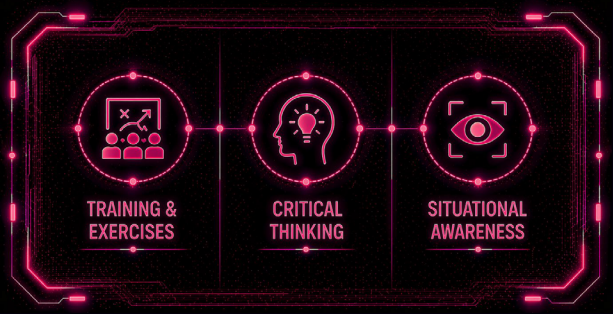
A particularly important aspect discussed was the role of governance. The effectiveness of CIMIC is closely tied to how governance systems function, whether they are transparent, accountable, and adaptive, or fragmented and unresponsive. The contribution suggested that future CIMIC models will depend on more dynamic forms of governance, capable of integrating diverse actors and responding to rapidly changing conditions. Examples from different regions illustrated how governance structures influence both the opportunities and limitations of civil-military cooperation.

Looking ahead, the contribution outlined a vision of CIMIC as part of a broader, technologyenabled system of societal resilience. This includes the use of digital platforms, AI-supported decision-making, and advanced capabilities in areas such as cyber and cognitive defence. At the same time, it emphasised the importance of civilian empowerment, continuous interactionbetween stakeholders, and the integration of human and technological resources.

In this perspective, CIMIC is no longer limited to supporting military operations, but becomes a central element in shaping how societies organise and defend themselves.

From a CIMIC perspective, this contribution points toward a future in which civil-military interaction becomes deeply embedded in how societies organise resilience and respond to hybrid threats. As cooperation expands across governance, technology, and societal structures, the challenge shifts from conceptual development to practical implementation. This raises an important question: if CIMIC is expected to connect such a wide range of actors and systems, how can it ensure that these complex networks remain functional and coordinated in practice, rather than becoming overly complex and difficult to manage during real-world crises?

Asset #15: Faultlines



ADAM WATERS
Director of AI Culture and Gaming, BFBS
Adam.Waters@bfbs.com

This contribution explored how crisis simulation and game-based approaches can be used to better prepare organisations for complex, fast-moving situations shaped by disinformation and internal friction. Using the FAULTLINES simulation as a central example, it placed participants in a high-pressure scenario where a deepfake video, appearing to show NATO forces firing on civilians, spreads rapidly online, forcing immediate coordination and response decisions before verification is possible.

What the contribution made clear is that crises of this kind are not only defined by external threats, but also by internal dynamics. While traditional wargaming often focuses on predicting adversary behaviour, this approach deliberately shifts attention inward. It highlights how competing priorities, hidden agendas, institutional constraints, and human behaviour within organisations can significantly shape outcomes. In the simulation, participants are assigned roles with both visible responsibilities and hidden motivations, creating tension and forcing them to navigate conflicting interests while still producing a coherent response.

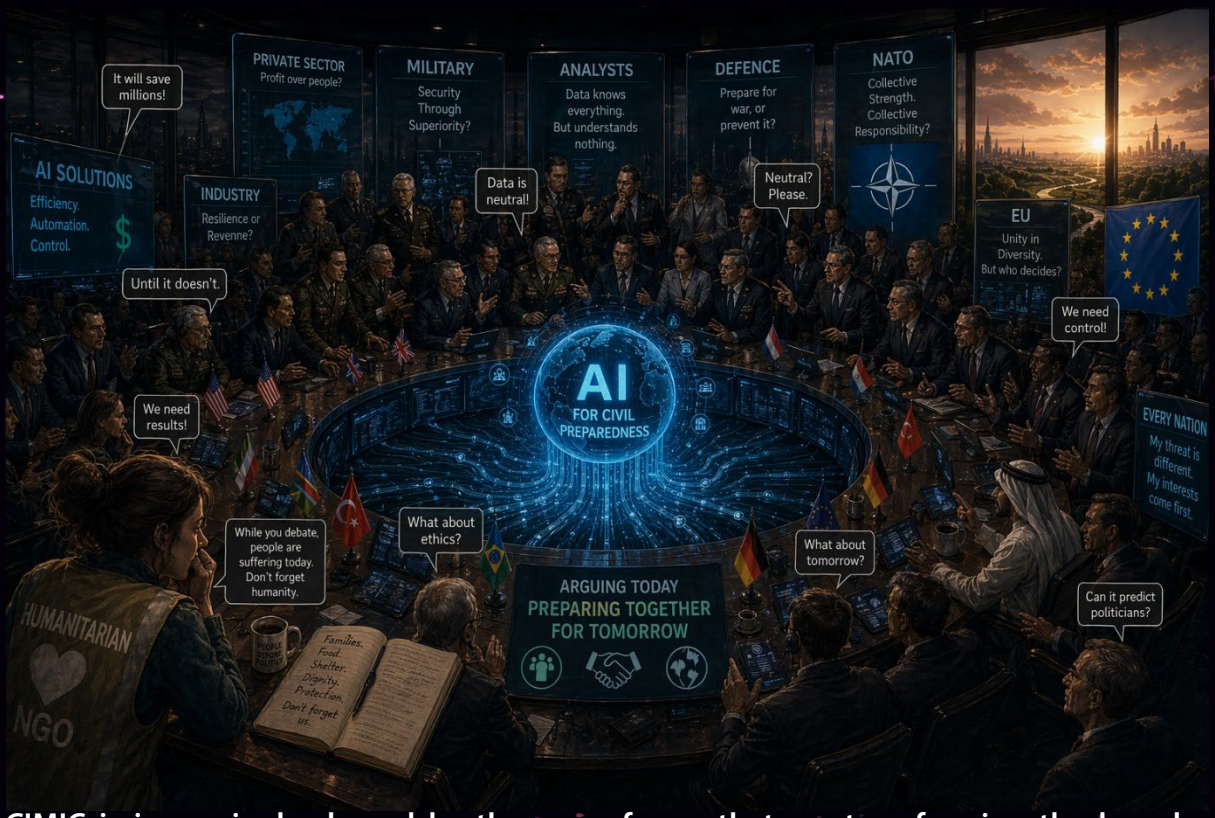
The structure of the simulation reinforces this complexity. Through time pressure, unexpected developments, and forced decision points, participants are required to act quickly, often with incomplete information. The introduction of "complication cards" further disrupts planning by injecting new constraints or shifting priorities mid-process. This design mirrors real-world conditions, where coordination is rarely linear and decisions must be made in the face of uncertainty, institutional friction, and external pressure from media or political actors.

A key insight from the contribution is that effective crisis response depends as much on understanding internal limitations as it does on anticipating external threats. Issues such as bureaucratic inertia, communication breakdowns, conflicting incentives, and information leaks can undermine even well-designed strategies. By making these factors visible within a controlled environment, the simulation allows participants to reflect on how their own organisations function under stress and where vulnerabilities lie.

At the same time, the contribution emphasised the value of experiential learning. Unlike purely theoretical discussions, simulations like FAULTLINES create a space where participants can actively engage with complexity, test decisions, and observe the consequences of their actions. The debriefing process, in which hidden motivations are revealed and decisions are reviewed, becomes a critical moment for learning, helping participants connect the simulated experience to real-world challenges.

In a CIMIC context, this contribution highlights the importance of preparing not only for external coordination but also for the internal dynamics that shape decision-making in multiactor environments. Civil-military interaction often takes place under pressure, with competing priorities and incomplete alignment, making it essential to understand how organisations actually behave in practice. This leads to an important question: if internal friction and competing agendas are inevitable in crisis situations, how can CIMIC structures be designed to manage these tensions effectively so that decision-making remains coherent and timely rather than fragmented under pressure?

Module 4: AI for Crisis Preparedness



CIMIC is increasingly shaped by the same forces that are transforming the broader security environment - and artificial intelligence is one of the most influential among them. From information analysis and decision-support to situational awareness and communication, AI is already embedded in how actors understand and respond to complex crises. In fast-moving environments defined by uncertainty and information overload, the ability to process data and derive actionable insights is becoming essential for effective cooperation.

At this stage, the discussion is no longer about whether AI should be acknowledged; it is already part of the operational reality. The real challenge has shifted toward understanding how to use it. This means knowing the available tools, recognising their limitations, and being able to define what is actually needed in a given situation. Using AI effectively is not about applying it everywhere, but about applying it meaningfully; selecting the right tools, asking the right questions, and integrating outputs into decision-making processes in a way that adds value rather than noise.

At the same time, AI raises important considerations around trust, transparency, and reliability, particularly in environments where civilian and military actors must share information and align decisions.Without a clear understanding of how these systems function, there is a risk of overreliance, misinterpretation, or fragmentation in how information is used across different actors. Recognising this shift, acaCIMICs included a dedicated panel on AI and emerging technologies, creating space not only for awareness, but for practical engagement. The discussion moved beyond general reflections and focused on how AI can be applied, what tools are relevant, and how they can support real-world tasks within CIMIC contexts.

The contributions within this panel brought together a range of perspectives that, while different in origin, pointed toward a shared reality. From the humanitarian side, INSO demonstrated how AI is already supporting operations through improved data collection, integration, and programme design. Their experience showed that while AI can significantly enhance situational awareness, it also introduces risks such as information overload and the potential manipulation of narratives, reminding us that more data does not automatically lead to better decisions.

The academic perspective from Leiden University added a critical layer to this discussion. By reflecting on the evolution of AI from game-based systems to today's generative tools, it challenged the tendency to overestimate current capabilities. AI can increase efficiency and support routine tasks, but it does not replace human judgement, especially in complex and unpredictable environments. The emphasis here was on responsible use, understanding when AI adds value and when it may limit deeper thinking or learning.

From a defence and strategic viewpoint, the focus shifted to implementation. The Estonian perspective made clear that the real issue is not technological capability, but coherence. AI tools for situational awareness, early warning, and decision support already exist, yet their effectiveness depends on how well they are integrated across fragmented systems. Differences between civilian and military actors, gaps between policy and operations, and challenges in data sharing mean that AI often exposes weaknesses rather than resolving them.

The private-sector contribution, represented by Microsoft, highlighted the scale and complexity of the digital infrastructure underlying modern security. With vast analytical capabilities and global threat visibility, industry plays a central role in detecting and responding to cyber threats. At the same time, this perspective underscored the importance of interoperability, data governance, and collaboration, as digital resilience increasingly depends on partnerships that extend beyond traditional institutional boundaries.

Across all these contributions, a common thread becomes clear: the challenge is no longer technological innovation, but the ability to align people, processes, and systems around it. AI is already present across humanitarian, academic, defence, and industry domains, but its impact depends on how coherently it is applied. Where systems are aligned, it can enhance coordination and decision-making; where they are not, it risks amplifying fragmentation and uncertainty.

In a CIMIC context, this convergence is particularly relevant. CIMIC operates at the intersection of these different domains, where information must be shared, interpreted, and acted upon across diverse actors. The discussion highlights that effective cooperation in the future will depend not only on access to advanced tools, but on the ability to use them collectively and with a shared understanding of their purpose and limitations.

This brings forward a broader reflection: with such a consistent set of insights pointing toward the same challenges, are we moving beyond acknowledging these issues and truly integrating them into how we prepare, coordinate, and act - or are we still at a stage where understanding is growing faster than implementation?

Asset # 4.1: INSO

Philip Riding, Deputy Director of Analysis and Research at INSO, focusing on responsible AI in humanitarian operations. INSO serve as the safety coordination and advisory body to the NGO community and provide daily support to more than 1,000 registered organisations working in high-risk contexts.

Alongside the United Nations Office for the Coordination of Humanitarian Affairs (UNOCHA) and the various local and international NGO platforms, they serve as an important pillar of the humanitarian coordination architecture.

Asset # 4.2: Game Research Lab, Leiden University

Mike Preuss is associate professor at LIACS, the Computer Science department of Leiden University. He is a member of the interdisciplinary research programme Society, Artificial Intelligence and Life Sciences (SAILS). Mike received his PhD in 2013 from the Chair of Algorithm Engineering at TU Dortmund, Germany, and was with ERCIS at the WWU Muenster, Germany, from 2013 to 2018. His research interests focus on the field of evolutionary algorithms for real-valued problems, namely on multi-modal and multi-objective optimization, and on computational intelligence and machine learning methods for computer games. He is also involved in Social Media Computing, and he was publications chair of the multi-disciplinary MISDOOM conference 2019.

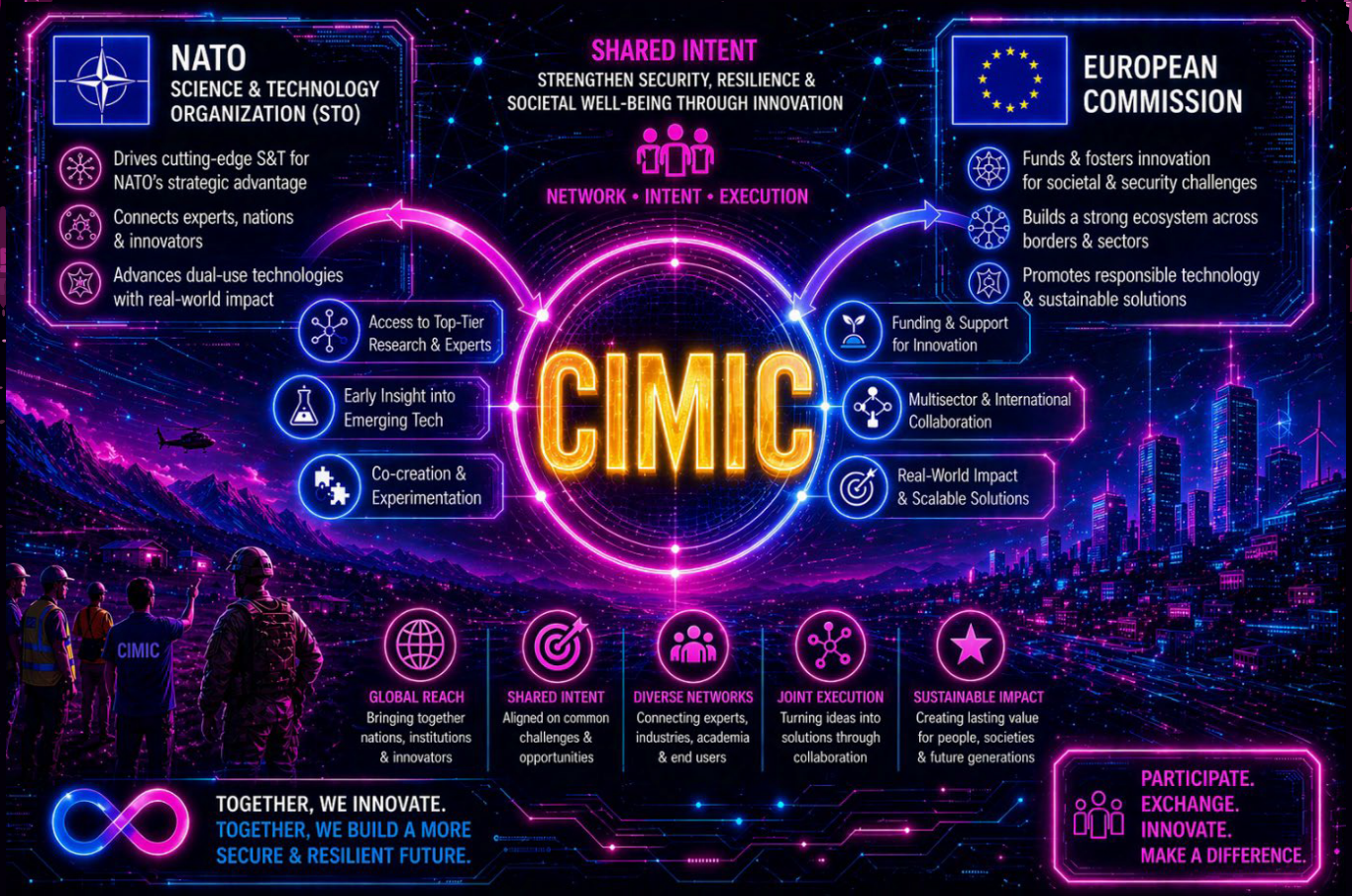
Asset # 4.3: Eva Sula, NATO DIANA Mentor

Eva Sula is a defence and security strategist working across NATO, EU, and national ecosystems, with a focus on civil–military cooperation and emerging technologies. She brings operational insight from the Baltic region and the Eastern flank, including lessons from Ukraine and regional resilience challenges.As a NATO DIANA Defence Mentor, she supports dual-use innovation and the adoption of new technologies into operational environments. Her work focuses on connecting policy, technology, and practitioners to strengthen preparedness, interoperability, and collective response.

Asset # 4.4: Microsoft

Rebekka Weiß, LL.M., is a fully qualified lawyer and Head of Regulatory Policy at Microsoft Germany. She leads projects and workstreams on data and competition policy, artificial intelligence, digital safety, and digital sovereignty. Previously, Rebekka worked at the digital association Bitkom from 2017, where she most recently led the department and team for Trust & Security. Rebekka studied law in Germany, Switzerland, and the United Kingdom and holds a Master of Laws in “Intellectual Property and the Digital Economy” from the University of Glasgow. She is co-editor of various legal journals and regularly publishes on the AI Act, data law, IT security law, and related legal fields.

Module 5: Accelerators



Including EU and NATO innovation actors in acaCIMICs reflects the reality that today's challenges cannot be addressed by operational actors alone. Civil-military cooperation increasingly depends on access to new technologies, shared knowledge, and evolving capabilities that are often developed outside the immediate operational environment. Institutions such as the European Commission's DG HOME and NATO's Science and Technology Organisation are key drivers behind these developments, shaping how innovation is funded, tested, and ultimately applied.

Bringing them into acaCIMICs is therefore not just about providing context—it is about opening the door. For many participants, these institutions can feel distant or difficult to access. By engaging with them directly, the audience gains a clearer understanding of what they actually offer: funding opportunities, research programmes, collaborative networks, and practical entry points for involvement. Whether through EU-funded projects, NATO research activities, or multinational partnerships, there are concrete ways for practitioners, researchers, and organisations to contribute and benefit.

At the same time, this exchange works both ways. It allows these institutions to better understand the needs and constraints of those working on the ground, helping to ensure that innovation is not developed in isolation but aligned with real operational requirements. In this sense, acaCIMICs becomes a space where connections are made—linking ideas, resources, andpeople - and where participants are not only informed, but also encouraged to engage, collaborate, and make use of the opportunities available.

Asset #5.1: NATO STO

NATO
SCIENCE & TECHNOLOGY ORGANIZATION

INSTITUTION	North Atlantic Treaty Organization
ORGANIZATION	NATO Science and Technology Organization
CORE ROLE	Provides scientific and technological expertise to support NATO's military and strategic objectives
PRIMARY MISSION	Maintain NATO's technological edge, interoperability, and innovation capacity in a changing security environment
STRATEGIC PURPOSE	Support deterrence, defence, and operational effectiveness through science and technology
OPERATIONAL SCOPE	Multi-domain (air, land, maritime, cyber, space, resilience, etc.)
MAIN ACTIVITIES	Collaborative research, technology development, knowledge exchange, education, and standardiation support
KEY APPROACH	Multinational collaboration between government, military, academia, industry, and NATO bodies
PARTICIPANTS	32 NATO Allies + partner nations, ~5000 scientists, multiple institutions
PROGRAMME STRUCTURE	Collaborative Programme of Work (CPoW) with ~450 ongoing activities
ORGANIZATIONAL STRUCTURE	Governed by the Science and Technology Board (STB), supported by Scientific and Technical Committees (STCs) and research activities
MAIN SCIENTIFIC DOMAINS	Systems analysis, human performance, sensing technologies, cyber & information systems (C5I), kinetic & non-kinetic effects, platform technologies, etc.
COLLABORATION MODEL	Nation-funded, voluntary participation with NATO coordination
ACTIVITY TYPES	Research Task Groups, workshops, symposia, technical courses, specialist meetings
OUTPUT TYPES	Technical reports, publications, standards, field trials, software, demonstrations, educational material
STANDARDIZATION ROLE	Contributes to NATO standards (via NATO Standardization Office – NSO)
INNOVATION FOCUS	Emerging and disruptive technologies (e.g. AI, cyber, quantum, autonomous systems)
EXAMPLE OUTCOMES	Interoperability frameworks, communication standards (5G/6G), autonomous systems integration, technology demonstrations
FUNDING MODEL	Primarily funded by participating nations; limited seed funding programmes
ENGAGEMENT MECHANISM	Participation through national coordinators, committees, and collaborative activities
LONG-TERM OBJECTIVE	Ensure NATO's scientific excellence, technological superiority, and operational advantage

Key takeaways:

- NATO STO acts as a collaborative network, connecting government, military, academia, and industry across the Alliance
- Focus on maintaining technological edge and interoperability in a rapidly evolving security environment
- Strong emphasis on emerging and disruptive technologies (e.g. cyber, AI, autonomous systems, quantum)
- Operates through a structured framework with Scientific and Technical Committees (STCs) aligned to capability areas
- Core mechanism is the Collaborative Programme of Work (CPoW) with multinational research activities
- Produces practical outputs: technical reports, standards, demonstrations, field trials, and training
- Contributes directly to NATO standardisation and capability development
- Based on a nation-driven funding model with NATO coordination
- Encourages knowledge sharing, innovation, and long-term scientific cooperation across Allies and partners

Asset #5.2: Horizon Funding Opportunities

EUROPEAN COMMISSION

INSTITUTION	European Commission
DIRECTORATE-GENERAL	DG HOME (Migration and Home Affairs)
CORE ROLE	Develops and implements EU policies on internal security, migration, and border management
PRIMARY MISSION	Ensure a secure, resilient, and well-managed European area of freedom, security, and justice
KEY POLICY AREAS	Migration & asylum, border security, counter-terrorism, crime prevention, cybersecurity, crisis management
OPERATIONAL ROLE	Strategic and coordinating body (non-operational)
MAIN FUNCTIONS	Policy development, legislative proposals, funding allocation, coordination among Member States, capability support
SECURITY APPROACH	Proactive, capability-driven, based on foresight, prevention, and preparedness
RESEARCH & INNOVATION ROLE	Oversees and funds security-related R&I programmes (e.g. Horizon Europe Cluster 3 "Civil Security for Society")
FUNDING INSTRUMENTS	Horizon Europe, Internal Security Fund (ISF), Border Management and Visa Instrument (BMVI), other EU funds
STAKEHOLDER ENGAGEMENT	Works with Member States, EU agencies, research institutions, industry, and practitioners
KEY PLATFORMS / NETWORKS	CERIS (Community for European Research and Innovation for Security), EU Innovation Hub for Internal Security
FOCUS ON CAPABILITIES	Supports development, testing, procurement, and deployment of security technologies and solutions
GOVERNANCE PRINCIPLES	Transparency, accountability, societal compatibility, respect for fundamental rights
STRATEGIC PRIORITIES	Strengthening EU security, enhancing resilience, safeguarding critical infrastructure, improving crisis preparedness
GEOGRAPHICAL SCOPE	European Union (with cooperation beyond EU where relevant)
LONG-TERM VISION	A secure and resilient EU supported by innovation, coordinated policies, and strong institutional cooperation

Key takeaways:

- DG HOME acts as a strategic enabler, linking policy, research, industry, and practitioners
- Horizon Europe Cluster 3 focuses on civil security through research and innovation
- Strong emphasis on capability development and real-world application, not just research
- Shift from reactive to proactive security through foresight and anticipation
- Creation of EU-wide ecosystems and networks (e.g. CERIS) to connect stakeholders
- Focus on societal compatibility, governance, and trust alongside technological innovation

Module 6: Node-X Roundtable Protocol