Civil-Military Cooperation and Hybrid Resilience in the European Union: Lessons from NATO Exercises

by Mabel Runyon

King's Policy Journal

KCL Policy Research Centre

Centre for European Affairs

Word Count: 2,318

January 2026

Civil Military Cooperation and Hybrid Resilience in the European Union: Lessons from NATO Exercises

I. Executive Summary

This policy analysis examines the implementation of civil-military cooperation (CIMIC) functions in recent NATO exercises and translates identified opportunities for enhancement into actionable policy recommendations that could strengthen EU-NATO resilience against hybrid threats. As a joint military function, civil-military cooperation facilitates collaboration between armed forces and civilian actors, integrating key civilian considerations into operations. As contemporary conflict grows more complex, threats continue to evolve, positioning civil military cooperation as a key mechanism for resilience. This analysis builds on the comprehensive assessments by the Civil-Military Cooperation Centre of Excellence (CCOE) on Steadfast Defender 2025 and Joint Cooperation 2025, which integrated critical CIMIC capabilities at the strategic and tactical level, informing commanders' decision making, supporting strategic planning, and much more. Following the exercises, military and civilian participants gave feedback through comprehensive assessments and analysis conducted by the CCOE, highlighting strengths and opportunities for improvement. The following policy recommendations seek to foster increased interoperability with enhanced EU-NATO preparedness frameworks, bolster CIMIC analysis and training through standardized programs, and strengthen alignment between NATO CIMIC and national structures. These recommendations aim to further strengthen partners' ability to anticipate and respond to hybrid threats with enhanced coordination and collaboration across civil and military domains.

II. Introduction

As hybrid warfare becomes more prevalent and advanced, addressing the challenges it presents have risen to be a top priority for the EU, the term hybrid warfare becoming a "staple of Europe's security policy vocabulary." (Giegerich, B. 2016.) With these threats increasingly targeting key civilian infrastructures, the need for increased civil-military cooperation has risen. Since the beginning of the war in Ukraine, the lines between war and peace have been blurred with the increasing incursions of hybrid threats on EU territory. Even prior to the war, hybrid attacks demonstrated a routine targeting of civilian infrastructure, crossing territorial lines, disrupting energy grids, communications, and undermining societal resilience (Edwards, Charlie. 2019.) This analysis identifies opportunities to strengthen coordination between military and civil crisis structures.

NATO's hybrid threat doctrine emphasizes the importance of resilience and early warning response mechanisms, particularly for those in CIMIC and J9 functions (NATO. 2025.) These functions remain largely active for during and post crisis liaison, while increasingly emphasizing forward looking,

preventative measures pre-crisis, including resilience and pre-conflict planning through integrating military strategies with civilian partners.

As previously mentioned, hybrid threats identify and target critical components to any state's wellbeing. The MCDC Countering Hybrid Warfare Project's work, *Understanding Hybrid Warfare* (MCDC. 2017) described them as 'the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects." Attacks such as these have been observed across the EU, including, but not limited to, the disruption and undermining of critical infrastructure, democratic processes, public services, and key government systems. Many of these tactics are used to weaken, influence or destabilize an opposing state, creating security challenges from the inside out. Hybrid threats can fall under the category of grey zone warfare, which is very difficult to succinctly define, as detailed by the UK Parliament's Defense in the Grey Zone report (UK Parliament, 2024). They specify, however, that the purpose of grey zone activity is to "Erode a state's ability to function specifically by operations below the threshold of direct state-on-state conflict." Actions such as these can inhabit a broad spectrum, often much more covert, but equally as destabilizing, utilizing tools such as cyber operations, disinformation campaigns, political interference, economic coercion, or territorial encroachments, "delivered directly by a state or through its proxies" the Parliament's report notes. These efforts are deliberately intended to interfere and disrupt, creating a consistent environment of strategic pressure and instability, thus testing a state's resilience and ability to effectively respond to threats.

This policy paper will analyze joint operational exercises on the strategic and tactical level to assess the effectiveness of current policies that integrate CIMIC techniques. CIMIC participation in these exercises is informed by NATO's article 3, which highlights civil preparedness and resilience as pillars for credible and enduring deterrence and defence (NATO, 2025). With hybrid attacks on the rise, re-evaluating vulnerabilities is critical for sustaining said resilience and responding to future threats.

III. Case studies

Recently, the NATO Civil Military Cooperation Centre of Excellence (CCOE) gathered data on exercises that provided findings that supported the evaluation of the role of CIMIC at both the strategic and tactical levels. Observing CIMIC methods in practice allows for NATO to explore opportunities for development and reinforce existing capabilities in coordination, civil impact modeling, or threat analysis that can then directly enhance resilience efforts. The CCOE's details collection and analysis of participant feedback provides invaluable insights into the operational application of CIMIC as well as a strong foundation for policy insights. Participants in the exercises were categorized into analysts (directly involved in exercises) and receivers (military and nonmilitary audiences of CIMIC efforts), using the NATO CIMIC Analysis and Assessment Capability (NCAAC). Research was carried out in

multiple forms: questionnaires, and direct interaction with exercise participants via interviews and observations. The first research phase addressed participant expectations, providing insights into the process of analysis and assessment. The second phase evaluated the NCAAC's effectiveness in enhancing the comprehension of civil factors within the operating environment (De Martin, Eleonora, et al, 2025). The research additionally aimed to understand how the NCAAC was implemented, based on previous field experience, which plays a significant role, determining both the level of expertise and participant bias. "Participants reported mixed awareness of NCAAC, which highlighted structural gaps and concerns in preparedness and training." According to the CCOE, "Evidence indicates that the implementation of NCAAC at both strategic and tactical level are at a very elementary stage. Only 19% of respondents are familiar with the Concept, 46% are aware but not familiar in practice, and 35% are not familiar at all." (De Martin, Eleonora, et al, 2025) These findings highlighted further opportunities to develop and improve assessment approaches, that support resilience.

Two critical cases were highlighted during the CCOE's assessment, the first being Steadfast Deterrence 2025, which examined CIMIC integration at the strategic level. Exercise Steadfast Deterrence aimed to enhance both deterrence and readiness across multiple domains, land, air, sea, cyber, and space, cyber being particularly critical for hybrid resilience. CIMIC participation in the exercise aimed to integrate a comprehensive civil environment picture into the Multi-Domain Strategic Operations Centre (MDSOC), support operation readiness, to provide civil environment inputs to Strategic Operations Planning Groups (SOPG's), incorporate civil factor considerations into the strategic battle rhythm and planning cycles, and to increase CIMIC support in deterrence and defense scenarios (De Martin, Eleonora, et al, 2025). The exercise demonstrated that CIMIC assessments are quite doctrinally sound, and well-integrated into exercise design; however, they suggested further opportunities to enhance CIMIC integration into strategic-level decision making. Key areas where capabilities could be further developed included a limited capacity to model the impact of operations on civilian networks and critical infrastructure, as well as the absence of clear early warning indicators and impact assessments to justify the activation of response measures (De Martin, Eleonora, et al, 2025). These factors become particularly relevant in the assessment of NATO's role within nationally owned resilience and emergency response frameworks, where alignment between NATO capabilities and national authorities remains uneven. The exercise additionally revealed a limited visibility of cross border civil response mechanisms, including access to the European Union's available tools and response measures. In sum, Steadfast Deterrence 2025 underscored the need to strengthen strategic level CIMIC analysis by improving civil impact modeling, early warning systems, and coordination with national and EU resilience structures.

Following this, Joint Cooperation Exercise 2025 (JOCO25) provided a valuable opportunity to assess the implementation of CIMIC into analytical frameworks under high tempo, multinational conditions. This exercise aimed to reinforce and strengthen cooperation and planning across forces,

with emphasis at the tactical level. The tactical level refers to the hands-on operations on the ground, led by commanders, putting strategic goals into practice. The exercise examined how CIMIC analysis is applied within brigades and divisions, revealing both operational strengths, and room to improve. JOCO25 evaluated CIMIC analytical support to commanders, particularly in terms of mission orientation. It tested reporting formats, analytical workflows, and different tools that can be used in deterrence and defense scenarios (De Martin, Eleonora, et al, 2025). Multiple findings emerged, particularly taking into account the multinational context. First, a lack of standardized reporting and guidance in place led to inefficiencies and divergencies across brigades. While commanders greatly valued CIMIC input, analyses were often undermined by time constraints and communication challenges. During the data collection phase, respondents highlighted that certain reporting formats risked introducing analytical bias, further complicated by the possibility that data obtained from civil sources could be intentionally or unintentionally compromised (De Martin, Eleonora, et al, 2025). Overall, JOCO25 demonstrated that while CIMIC analysis is operationally valued at the tactical level, its effectiveness in multinational and high tempo environments is often constrained by inconsistent standards, time limitations, and data reliability, underscoring the increasing need for more interoperable analytical frameworks.

IV. Policy recommendations

NATO's current policies that support civil military cooperation are already extensive, and highly effective. Within this ongoing effort, NATO has recently conceptualized Counter Hybrid Support Teams. These are teams made-up of civilian experts who can incorporate military advisory support, intended for both crisis and capacity building which extends to pre-crisis measures, enhancing and reinforcing the Allies' ability to strengthen resilience against hybrid threats. Its one of the first formal ways for NATO to provide expert civil military support in this domain (NATO, 2025). To compliment these efforts, recommendations within this paper build on the valuable findings and lessons from the CCOE, enhancing NATO and EU CIMIC capabilities. This paper proposes three policies that could address challenges and support further development as identified during recent CIMIC and NCAAC engagement within NATO exercises.

First, to enhance coordination and compliment recent initiatives, NATO and the EU might consider the implementation of a formalized, hybrid preparedness assessment framework that aligns NCACC and CIMIC analysis methods with EU resilience planning. Based on the CCOE's findings, fragmented information flows, inconsistent indicators and challenges of alignment between the EU, and NATO make CIMIC NCAAC processes more difficult, uneven, and less effective. While NATO and the EU maintain parallel resilience frameworks, no formalized mechanism currently aligns CIMIC and NCAAC derived assessments with EU resilience planning across multiple domains. CIMIC analysis,

on the strategic level, increasingly addresses resilience, particularly in the civilian domain, highlighting infrastructure for example, an area where the EU has pre-existing policies and frameworks (Migration and Home Affairs, 2023). The integration of an EU-NATO hybrid preparedness assessment framework would simultaneously coordinate, reinforce, and align NATO CIMIC and EU resilience measures. This initiative would support resilience within infrastructure, civil, and cyber domains, enhancing increasingly interoperable formats that would streamline EU and NATO goals. This would improve long-term cohesion and strategic foresight while ensuring that NATO CIMIC methods directly support EU resilience efforts.

Second, the development of a standardized CIMIC analytical professionalization pathway that's accredited and aligned with NCAAC standards and could support more coordinated responses to hybrid threats. Exercises Steadfast Deterrence and Joint Cooperation revealed inconsistencies in the analysts implementing NCAAC, with some not holding a professional analytical background (De Martin, Eleonora, et al, 2025). While existing CIMIC training remains effective and thorough, some work has yet been done to ensure a standardized skillset with accreditation for CIMIC analysts, other than those who have gone through formal training at the CCOE. Effectively assessing both tactical and strategic exercises across domains requires different competencies and capabilities, thus shedding light on the need for increasingly standardized training to ensure consistent assessments and analyses. This pathway, guided by policy, would align with NCAAC and the CCOE, integrating EU analysts. These programs would include (but not limited to) training in hybrid and multi-domain analysis, information environment assessment, and assessment based on level-specific needs (tactical, operational, strategic). This would build a standardized and shared analytical framework between the EU and NATO analytical communities, supporting the quality and efficiency of analysis and decision support within multi-domain operations when it's needed most.

Finally, NATO and the EU may consider adopting policies that promote the integration of CIMIC and NCAAC derived assessments into EU national resilience frameworks, in cooperation with willing allied states. The exercises reviewed in this analysis demonstrated fragmented information flow and limited interoperability between NATO CIMIC structures and nationally owned civil emergency response frameworks. This would support national preparedness, contingency planning, and critical information sharing that could benefit both parties. By supporting national frameworks with CIMIC analysis methods, national risk assessment could be bolstered and supported by NATO experts, reinforcing resilience against hybrid threats. Having CIMIC analysis support national resilience structures would strengthen preparedness across critical civilian domains while maintaining consistent alignment with EU instruments.

V. Conclusion

This policy analysis demonstrates that recent NATO exercises, Steadfast Deterrence 2025 and Joint Cooperation 2025, informed by assessments conducted by the NATO CCOE, confirmed the value of CIMIC capabilities at the strategic and tactical operational levels. The integration of CIMIC functions in these exercises supported key decision making, contributed to strategic planning, and significantly enhanced critical situational awareness in complex, multi-domain environments. At the same time, following the exercise, feedback from military and civilian participants highlighted potential enhancements to existing capabilities through increased analytical standardization, training coherence, and integration and cooperation within EU national structures. Incorporating these lessons into policy considerations can help reinforce EU-NATO resilience against hybrid threats.

These recommendations outlined in this analysis provide frameworks to identify these challenges while supporting interoperability, strengthening CIMIC analysis, and aligning resilience frameworks across the EU and NATO. Incorporating these measures can help reinforce civil military cooperation, support analytical effectiveness, and ensure, particularly in an age when its needed most, that CIMIC capabilities are consistently integrated as a core pillar of collective defense and national resilience measures.

Bibliography:

Giegerich, B. (2016). Hybrid Warfare and the Changing Character of Conflict on JSTOR. *Jstor.org*, *15*(2). https://doi.org/10.2307/26326440

NATO. (2025). *Resilience, civil preparedness and Article 3*. Site Name Seo. https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

NATO. (2025a). *Countering hybrid threats*. Site Name Seo. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

Dr. Cullen, P. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

De Martin, E., et al. (2025). *Advancing NATO CIMIC analysis and assessment capability: Insights from tactical and strategic level exercises*. NATO Civil-Military Cooperation Centre of Excellence, pp. 1–21.

Defence in the Grey Zone. (2024). Parliament.uk. https://publications.parliament.uk/pa/cm5901/cmselect/cmdfence/405/report.html

Edwards, C. (2019). *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. IISS. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

Ministry of Defence. (2018, November 19). *Allied Joint Doctrine for Civil-Military Cooperation (AJP-3.19)*. GOV.UK. https://www.gov.uk/government/publications/allied-joint-doctrine-for-civil-military-cooperation-ajp-319

NATO. (2023, December 12). *Cyber Defence – NATO's ACT*. https://www.act.nato.int/activities/cyber/

Critical infrastructure resilience at EU-level. (2023b). Migration and Home Affairs. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en