Civil-Military Cooperation
Centre of Excellence

FACTSHEET

CIMIC in the Cyberspace Domain

Concepts, Interoperability and Capabilities Branch
2025

INTRODUCTION

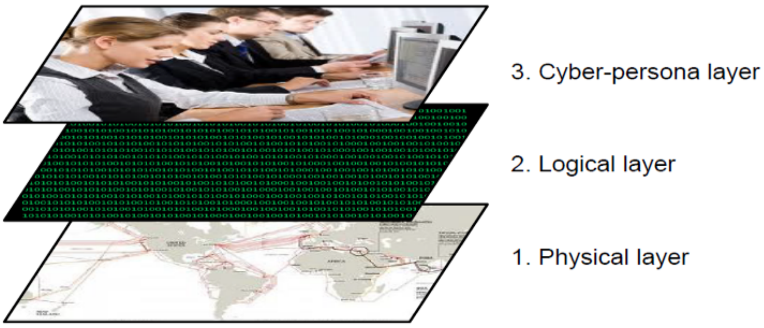
Civil-military cooperation (CIMIC) is described in AJP-01 Allied Joint Doctrine as part of the Joint Function Framework. As a Joint Function, CIMIC must be recognized in every domain of operations and in all effects dimensions — physical, virtual, and cognitive. This publication aims to explain the relationship between CIMIC and the cyberspace domain, providing examples for clarification.

NATO defines cyberspace as the global domain consisting of all interconnected communication, information technology, and other electronic systems, networks and their data, including those that are separated or independent, which process, store or transmit data.[1]

CYBERSPACE ENVIRONMENT

The cyberspace environment is far more than merely the internet but extends to operational technology (OT) or military command and control systems that are air gapped from the internet. It is not limited to, but at its core consists of, a computerized environment, artificially constructed and constantly under development. This includes networks and devices connected by wired as well as wireless connections, which means that cyberspace, like other domains, depends on the unobstructed use of the electromagnetic spectrum.

Cyberspace infrastructure is largely globally interconnected; however, geographic boundaries do apply in the context of jurisdiction, with national responsibilities. This is why assigning classical operational boundaries in cyberspace and attribution of activities to a cyber threat actor or nation state are particularly difficult. Cyberspace is also distinct in that its underlying physical elements are entirely human-made, different from land, sea, air, and space – this implies that 'the map' can change more easily and its higher layers are rather characterized by interests than geographical and political borders.



All devices reachable via cyberspace could be potential targets and potential threats. Risks in cyberspace may be managed through the manipulation of the domain itself, but preparation and mitigation should also take into account the other domains, e.g., primary – alternate – contingency – emergency ('PACE') plans for communications that do not solely rely on cyberspace capabilities. According to AJP-3.20 cyberspace consists of three layers: physical, logical and cyber-persona.

[1] NATOTerm, NATO Terminology Database, NATO agreed definition.

THREATS AND DISRUPTIONS

Strategic competitors test the Alliance's resilience and seek to exploit the openness, interconnectedness and digitalization of allied nations, knowing that their critical national infrastructure but also democratic processes largely rely on computers. They interfere with our societies' democratic processes and institutions, and they target the security of our citizens through hybrid tactics and malicious activities in cyberspace. However, this rarely happens in the open but through proxy (cyber threat) actors, and on top, hostile intelligence services recruit insiders through traditional intelligence methods. These hybrid tactics leave democratic societies in a dilemma because they ultimately have to respond openly to covert malicious activities performed with plausible deniability bound to their legislation.

NEW OPPORTUNITIES – NEW RISKS

The ever faster development of information technology, including machine learning and artificial intelligence, building on evolving and disrupting technologies, opens up new risks as well as new opportunities. While these developments create new vulnerabilities and potential for malicious activities, at the same time, there is potential to develop better protection, resilience, and new opportunities for counter-attacks. Both our socities in general and the military in particular rely on the free and responsible use of cyberspace. This arguably renders cyberspace the most 'civilian' of all domains. Those militaries that best integrate and use the capabilities and capacities of the civil society, particularly non-military academics, science, and the private sector, will likely be able to out-pace and out-excel adversaries.

CIVIL-MILITARY INTERDEPENDENCIES

Most of cyberspace, throughout its physical, logical, and cyber-persona layers, is built, owned, and run by non-military actors. Adversaries predominantly use hybrid activities and prepositioning in our critical infrastructures to challenge and degrade the Alliance's resilience and destabilize our societies. Therefore, NATO's comprehensive approach to deterrence and defense is especially relevant in cyberspace. Cyber defense is a whole-of-society challenge that can only succeed through integrating non-military potential, capacities and capabilities.

CIMIC IN THE CYBERSPACE DOMAIN

NATO differentiates between defensive cyberspace operations (DCO) and offensive cyberspace operations (OCO). DCO are defined as defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace. OCO are actions in or through cyberspace that project power to create effects which achieve military objectives.

While building up its own NATO capabilities, the Alliance also strongly relies on Allies' capabilities, particularly for offensive activities, taking into account that, though effects are hardly limited to geographical boundaries, the employment of capabilities is subject to national legislation and caveats. The desired, collateral, and third-order effects of COs may impact all layers of cyberspace or, ultimately, outside of cyberspace. COs may affect human sense and decision-making and may be used or misused to influence behavior. Likewise, COs may also affect physical entities outside of cyberspace and vice versa.[2]

The reciprocity of activities and effects between cyberspace and the other operational domains necessitates fully integrating cyber operations into the multi-domain operations (MDO) approach. To ensure the comprehensive use of military and non-military effectors, the synchronization of military and non-military cyberspace activities demands intensive and effective civil-military interaction (CMI) informed by a comprehensive civil factor integration (CFI).

NATO is in the process of establishing a new NATO Integrated Cyber Defence Center (NICC) collocated with its Supreme Headquarters Allied Powers in Europe (SHAPE) in Mons, Belgium.[3] The NICC will enhance network protection, situational understanding, and the implementation of cyberspace as an operational domain throughout peacetime, crisis, and conflict, and will thus be beneficial to both NATO and Allies.

In the NICC, civilian and military experts from relevant NATO bodies and allied nations will work side by side. It aims to integrate industry and academia, ensuring 24/7 visibility over NATO Enterprise networks, as well as other networks beyond, where incidents could risk impacting military operations in the Euro-Atlantic area.

Acknowledging the civilian dominance in cyberspace requires the NICC to integrate a solid CIMIC capability performing its core activities CFI and CMI. Doing so will enable the NICC to efficiently synchronise military and non-military activities in cyberspace. It will be of particular importance to explore how CIMIC knowledge and processes can facilitate the interaction with national liaisons, industry and academia beyond a traditional 'quid pro quo' contracting.

The core of CIMIC capabilities enabling military success in cyberspace activities will be their people. Well trained analysts and personnel specialized for the liaison and collaboration with non-military actors will be key to success. Effective cooperation demands not merely cyber expertise. Cyber CIMIC personnel will have to have knowledge of civil governance, understanding of players in the commercial sector and most of all intercultural competence to navigate the diversity of actors involved.

[2] AJP-3.20; Activities outside of cyberspace which have an effect on cyberspace, are not considered COs, e.g. dropping a bomb on CIS.

[3] James Appathurai, NATO Deputy Assistant General for Innovation, Hybrid and Cyber, in: Martin, A. Recorded Future News

REFERENCES

NATO 2022 Strategic Concept, 29jun2022.

MC 0665, 12 June 2018, Military Vision and Strategy on Cyberspace as a Domain of Operations.

AJP-01 Edition F Version 1, December 2022: Allied Joint Doctrine

AJP-3.20 Edition A Version 1, January 2020: Allied Joint Doctrine for Cyberspace Operations.

NATOTerm, NATO Terminology Database

Martin, Alexander, Recorded Future News: Appathurai, James, NATO Deputy Assistant Secretary General for Innovation, Hybrid and Cyber (https://therecord.media/nato-new-military-civilian-cyber-center-mons-belgium).