If You See Something, Say Something:

Civil Affairs and the Dual-Lane Integration of Civilian-Generated Information Across the Competition Continuum

Major Shannon Woodman

After February 2022, Ukraine turned its population into an information-collection network at operational scale. Platforms such as eVorog and ePPO verified hundreds of thousands of citizen reporters through the Diia digital-identity system and delivered their reports to military users within minutes. The effort also exposed issues such as analyst overload, deliberate adversary poisoning of the network, and unresolved legal exposure for civilian reporters.

U.S. Army doctrine does not lack a framework for assessing this information, but it divides it in two. Civil Affairs owns civil knowledge integration (CKI) for information about the civil component, and military intelligence owns information related to threats and the enemy. ATP 3-57.50 keeps the two apart: "CKI is not an intelligence activity." A civilian report of enemy activity finds the seam between them, though. CKI excludes it by content, and the intelligence process can take it in only as an unrated first-time source, which ATP 2-22.9 rates F/8, or "cannot be judged."

The paper recommends formalizing the dual-lane architecture that doctrine already implies, with Civil Affairs as lead integrator for persistent civil-information reporting. What a report is about decides its lane, not when it arrives. Civil information remains CA's, and threat content stays with intelligence oversight, from competition through conflict.

Predefined triggers set how deliberately the network is tasked toward threat reporting, working as a dial rather than a switch, because a reporter's legal exposure rises with how directly the channel feeds military use. Civil network development and engagement (CNDE) develops the network, while CKI validates its reporting, and CMI integrates it. A CA-owned reporter registry lets reporters cross into intelligence channels with a track record instead of at F/8.

Separating the lanes also limits legal risk under the U.S. Law of War Manual and protects CA access, which doctrine already warns is lost when CA is associated with intelligence gathering.

Ukraine is unfortunately the easiest version of this problem to understand. Abroad, CA cannot assume a national identity system, a unified population, or a trusted state. Validation therefore shifts from the report to the reporter: from volume to verifiable position, relationship history, and motive assessment that screens out local denunciation as well as adversary deception. As the app Watch Duty shows domestically, a trusted validation network matters more than the collection technology.

Most of the paper's recommended DOTMLPF-P changes fall in policy and doctrine. They include defining how a civil-network report crosses into intelligence channels, aligning CA and intelligence reliability ratings, and fielding a platform-agnostic registry, rather than simply buying new software.