



The Front We Cannot See

Cognitive warfare has reached the Eastern Mediterranean, and much of the answer to it is already European.

Celia D. Hanley

(Founder and President of Catalina Intelligent Solutions LLC (CatalinaIQ). A former Senior Operations Officer of the Central Intelligence Agency and the Defense Intelligence Agency, with over forty years in clandestine operations, counterintelligence, and international security, she now develops cognitive security and risk mitigation programs for private-sector, government, and academic audiences.

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. Government. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or endorsement of the author's views.

Copyright: @ 2026 Research Institute for European and American Studies (www.rieas.gr)

Publication date: 14 August 2026

Note: The article reflects the opinion of the author and not necessarily the views of the Research Institute for European and American Studies

A migrant surge builds at a European land border, organized not by desperation alone but by a neighboring state that decided to open the gate. GPS signals fall across civilian airspace over the Eastern Mediterranean. An undersea cable is severed. A manufactured story about a national leader spread faster than any correction can chase it. In most ministries, and most newspapers, each of these is filed as a separate problem: migration, aviation safety, infrastructure protection,

disinformation. They are not separate. They are instruments of one campaign, aimed at a single target that no border fence or air-defense battery is built to protect: the cohesion of European societies and the trust that holds them together. That campaign has a name. It is a cognitive warfare, and Europe's southeastern edge is one of its most active fronts.

Cognitive warfare is not cyberwar, and it is not the old business of propaganda. Cyber operations attack the network; cognitive operations attack the mind that reads the screen. Propaganda tried to make you believe something. Cognitive warfare, in its most effective modern form, tries to make you unable to believe anything with confidence. Russia's doctrine calls this Reflexive Control: the deliverable manufacture of epistemic disorder, a condition in which government, a company, or an electorate can no longer reliably tell what is true about its own situation, and therefore cannot act. China pursues a quieter version through its Three Warfares (public-opinion, psychological and legal), engineered less to create chaos than to bend decisions toward Beijing's interests. The 2026 U.S. Annual Threat Assessment describes both, in plain language, as active operations, now running at a scale that artificial intelligence has made almost free.

That last point is what should concern a reader most. The cost of running these operations has collapsed. A synthetic video, a fabricated document, a coordinated swarm of inauthentic accounts, a few hundred euros paid over Telegram to a local proxy to light a fire or move a crowd: each is the information-domain equivalent of a cheap drone flown at a multimillion-euro interceptor. The math does not favor the defender. And the Eastern Mediterranean offers an adversary an unusually rich set of seams to work. Contested maritime boundaries, energy corridors, an exposed migration frontier, and decades of historically charged narratives between neighbors all require no intervention, only amplification. Moscow does not need to fabricate a Greek-Turkish grievance. It needs only to find one and pour accelerant on it, at a moment of its own choosing, for almost nothing.

Europe's problem is not that it lacks capability. It is that the capability is aimed at the wrong layer. Cybersecurity agencies defend the network. Border services defend the frontier. Counterterrorism units defend against violence. Each owns a fragment of the threat, and none owns the whole, because the whole is not technical, territorial, or kinetic. It is cognitive, and it moves across all three at once. A national security-operations center will detect an intrusion. It will not detect a narrative, timed to an election or a border crisis, designed to make a population doubt its own institutions. That is the architecture gap, and it is the gap the adversary was built to exploit.

There is a model that works, and it is already largely European. Sweden's Psychological Defence Agency, established in 2022, treats the information environment as terrain to be defended deliberately and lawfully, in partnership with an informed public rather than over its head. NATO's Allied Command Transformation now speaks openly of cognitive defense as a mission.

The encouraging fact is that this defense is cheap, a rounding error next to a fighter wing, and it unites high-spending and low-spending states alike, because every one of them is already a target. The cautionary fact is that the same tools can be turned inward. A cognitive-defense capability without legal guardrails, distinguishing the defense of the public square from the capture of it, becomes in the wrong hands an instrument of exactly the manipulation it was meant to stop. Any serious architecture has to be built with that line drawn first, in law, not discovered later.

Defense of this kind cannot be purely reactive. By the time a false story has been fact-checked, it has already done its work: the correction reaches a fraction of the original audience and arrives after the decision it was meant to inform. The more promising approach borrows from medicine. Inoculation theory holds that briefly exposing people to a weakened, clearly labeled dose of a manipulation technique, showing them how the trick works before they meet it in the wild, lets them build their own resistance, much as a vaccine primes the immune system. Delivered at scale, this is called pre-bunking, and its strength is that it targets the method rather than any single lie. An audience taught to recognize manufactured outrage, or the signature of a coordinated amplification campaign, is protected against the next operation as well as the last. Here again, Europe has been among the most serious adopters, which is one more reason the continent is much better positioned than it might assume.

Nowhere are the stakes clearer than in the Eastern Mediterranean, where the raw material of cognitive warfare is abundant and the tools to exploit it are cheap. A rumor about a maritime incident, a doctored image from a contested island, an amplified claim about a bilateral deal: each can move opinion in Athens, Nicosia, or Ankara faster than any ministry can answer, and each costs its author almost nothing. This is not hypothetical. In late 2024, a NATO and EU member, Romania, watched its constitutional court annul a first-round presidential result after evidence of a coordinated online amplification campaign surfaced, the first time a European democracy voided a national vote over manipulation of the information environment. The precedent should concentrate minds and resolve across the region. The contest is not coming. It is here, and it is already shaping outcomes.

The real frontier in the Eastern Mediterranean is not the Evros River, nor a line drawn across the Aegean. It is the far shorter distance between what a society perceives and what is actually true. That is the ground now under attack, and the West has spent a generation learning to defend everything except it. The good news is that this front, unlike the others, can be held for the cost of deciding it is worth holding.