From Shield to Sword: The Two Edges of Europe's New Strategy

Europe has decided that defending is no longer enough. The strategy it is reaching for has two edges, and one of them can be taken up now, at low cost, by nearly everyone already in the fight.

By 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. This article is based entirely on open-source, unclassified information.

Publication date: 7 September 2026

Something has shifted in how Europe talks about hybrid threats. For most of the past decade the language was defensive: resilience, situational awareness, protection of critical infrastructure. In the first months of 2026 that changed. The European Council on Foreign Relations published a strategy titled from shield to sword. On 16 March 2026 the Council of the European Union committed the bloc to prevent, deter, and respond to hybrid campaigns irrespective of their origin, scale and intensity, and weeks earlier it had sanctioned six individuals for information manipulation. Italy's defense minister proposed a national cyber force and an EU-level body to command counter-hybrid operations. The judgment behind the shift is sound. A campaign that produced a fourfold rise in sabotage across the continent, and 321 suspected incidents in Germany alone in a single year, has not been slowed by defense on its own. Europe is right to reach for the sword.

A great deal now rests on a single word, and the word is offensive. It carries two meanings that the current debate tends to run together, and pulling them apart is the difference between a strategy Europe can act on immediately and one that will stall in argument. Offensive can mean acting first, moving before the adversary's operation lands rather than cleaning up after it. It can also mean acting against the adversary, striking at its people or its systems. The first is a question of timing. The second is a question of target. They are not the same decision, and they do not carry the same cost, the same legality, or the same answer to who is permitted to carry them out.

Hold those two questions apart and the path forward becomes clear. The most valuable moves available to Europe are the ones that act first while still aiming only at Europe's own defense, never at the adversary, and two of them are ready to use today. The first is prebunking: teaching a population to recognize a manipulation technique before the adversary deploys it, much as a vaccine prepares the body before it meets the disease. Prebunking acts first, which is what makes it feel like offense, yet it targets no one abroad. It works entirely on the resilience of the audience at home. The second is attribution: exposing a coordinated operation publicly and in detail. Attribution imposes a genuine cost, because a network that has been named and documented can no longer do its job and usually cannot be reused, and it does so without touching a single adversary system. It defeats the operation by describing it accurately, in public, and any government, company, or newsroom is free to do it. Together, prebunking and attribution deliver most of the initiative Europe is asking for, they require no special authority, and they carry no risk of escalation.

The second meaning of offense, striking directly at the adversary, sits on the far side of a line that every European state already draws inside its own laws. Degrading an opponent's information infrastructure, taking down its networks, or interfering with its systems is state action. It belongs to defense ministries, intelligence services, and national cyber forces acting under national authority and oversight, which is precisely where Italy's proposed cyber force would sit. It does not belong to a media-literacy program, an electoral commission, or a corporate security team, and the hazard of one word covering both meanings is that it quietly draws those civilian bodies toward activity that was never theirs to conduct. Keeping the two edges distinct is how each country keeps its own counter-hybrid coalition on the right side of its own law.

There is a further reason to keep the line sharp, and it is operational as much as legal. In the contest over information, credibility is the whole capability. An organization whose attribution is trusted can end an operation with a single well-sourced report. The moment that same organization is found to have crossed into disrupting networks or manipulating systems, its credibility collapses, because its audience can no longer tell an honest exposure of the adversary from an operation of its own. Exposure and disruption are not two settings on one dial where more is always stronger. A hard line runs between them, and crossing it does not make a cognitive defense more aggressive. It disarms it. A serious architecture names that line, holds its civilian and private tiers firmly on the exposure side, and reserves disruption to the state bodies built and supervised to carry it, with their lawyers and their oversight in the room from the start.

This separation also settles an argument that has slowed Europe's response. Skeptics of a cost-imposition strategy point out, fairly, that raising costs only deters if it changes the adversary's calculations, and that no European capital can read Moscow's calculations well enough to be certain it will. That objection bites hard against the second edge, where the whole theory depends on the adversary being deterred. It does not touch the first edge at all. Prebunking does not require Moscow to be deterred; it strengthens the European public whatever Moscow decides. Attribution does not require Moscow to be deterred; it destroys the specific operation whether or not the next one is discouraged. The strongest actions available to Europe are exactly the ones that do not depend on winning a debate about the adversary's state of mind, a debate Europe cannot win. That is not a reason for caution. It is a reason to move first, where moving first is cheapest and asks the least permission.

The decade of defense that Europe is now moving beyond was not a failure of effort or of will. It was a mismatch. Europe brought the tools of protection to a contest being fought over perception, and protection was never built to win that contest. The correction now under way is the right one, provided Europe is clear about the instrument it has chosen. A sword has two edges. The first, acting ahead of the adversary to inoculate the public and to expose the operation, can be taken up today, by a broad coalition, at low cost, under authority that already exists, and it delivers most of what the move from shield to sword is actually reaching for. The second, striking at the adversary's own systems, belongs to states under oversight and has to be walled off from the rest by a line drawn in law before anyone lays a hand on it. The choice in front of Europe is not between the two edges. It is to take up the first without delay, and to approach the second only once the line that governs it has been drawn. Knowing which edge you are holding is not a footnote to the strategy. It is the strategy.