

Hybrid warfare is one of those terms that manages to capture the mood of an era. It describes a form of conflict that is neither quite war nor quite peace: a condition in which power is exercised through a web of actions that may look trivial in isolation but together build strategic pressure. It is a method that has only really become visible now that Europe has been forced to live with it.

An old pattern in a new shape

Mixing regular and irregular means is nothing new. History is full of actors who avoided open battle and instead struck at logistics, public opinion and political structures. What is new is not the mixture itself but the analytical attention now paid to it. When researchers in the early 2000s began describing conflicts in which conventional capabilities, guerrilla tactics, terrorism and organised crime were coordinated, they were trying to capture a changed reality — one in which the synergy between methods mattered more than the methods themselves.

Since then, though, the term has drifted away from the battlefield. Today it refers just as much to the political grey zone: the space in which states try to shift the balance of power through small, deniable steps, each one too minor to trigger a military response, but which together alter the strategic balance.

The grey zone as method

The grey zone is a strategic space built on ambiguity. Those who operate there want to avoid crossing the threshold that would trigger a formal armed response, while still constraining their opponent's freedom of action. That might mean probing borders, sowing uncertainty, exploiting legal loopholes, or simply grinding down institutions until they start to buckle. It is a form of political warfare that needs no uniforms to be effective.

Western debate has sometimes wanted to see a single, coherent doctrine behind all this. The reality is messier. Some operations are coordinated, others opportunistic. Some follow a clear strategic line, others are improvised and only fitted into a pattern after the fact. Crediting an adversary with too much coherence is one mistake; treating every incident as isolated is another.

Europe after 2014

The annexation of Crimea was a turning point. It was carried out using unmarked soldiers, information operations, economic pressure and cyberattacks — a combination deliberately kept below the threshold that would have been crossed by regular troops marching in under a flag. It showed just how quickly facts on the ground can change when ambiguity itself becomes part of the toolkit.

Since the full-scale invasion of Ukraine, hybrid activity has increasingly targeted Europe directly. The aim has been to sow uncertainty, divide allies and erode support for Ukraine. The methods are familiar: disinformation, sabotage, economic coercion, proxy actors. What has changed is the frequency and the low bar for risk-taking. One-off agents are recruited for single tasks, often through social media, which makes attribution harder and the political cost of getting caught lower.

The Baltic Sea's murky floor

The Baltic Sea has become a map of the grey zone. In recent years, undersea cables and pipelines have been damaged on several occasions. Ships have been spotted nearby, anchors have been dragged across the seabed, and suspicions have run high politically — yet the evidence has usually fallen short of what is needed for a conviction. The pattern repeats: physical damage, a ship in the vicinity, political suspicion, insufficient proof.

It is precisely this ambiguity that makes the tactic work. The damage is real, but intent is hard to prove. Meanwhile, a growing shadow fleet of tankers with murky ownership moves through the region, further blurring the line between civilian and military activity. GPS jamming from Russian transmitters has disrupted tens of thousands of flights and become part of a sustained, low-level pressure campaign against critical infrastructure.

The porous walls of the information space

Information manipulation is the cheapest arena for hybrid activity. In recent years, networks have sprung up that clone legitimate news sites and fill them with slanted or fabricated stories. The goal is to undermine support for Ukraine, influence elections and breed distrust in institutions. It does not take advanced technology — just persistence and a working understanding of how digital ecosystems operate.

At a time when information travels faster than anyone's ability to verify it, the information space becomes a battlefield in its own right. Whoever succeeds in sowing doubt does not need to win the argument — weakening trust is enough.

Migration, sabotage and proxy actors

Migration has repeatedly been used as a lever. Pushing people towards borders creates political dilemmas that can then be exploited in the next narrative. Sabotage, meanwhile, has often been carried out by people with no intelligence background at all — recruited for a single job via messaging apps. It can mean arson, parcel bombs, or simply mapping out defence industry sites.

It is a method that deliberately blurs the line between crime, accident and deliberate attack. That uncertainty is itself part of the toolkit.

China's parallel grey zone

China runs its own version of grey-zone tactics in Asia: coastguard vessels, maritime militia, artificial islands and economic leverage. The goal is to establish irreversible facts on the ground without triggering open war. In the Baltic Sea, Chinese-flagged vessels have turned up in cable-damage incidents too, showing how attribution gets even harder once multiple actors start operating in the same grey zone.

Europe's and Sweden's response

The EU and NATO have built up structures to deal with hybrid threats: shared frameworks, toolboxes, intelligence functions and exercises. Sweden, for its part, has strengthened its total defence concept, set up an agency for psychological defence, and tasked sector authorities with improving situational awareness and information-sharing.

The strength lies in a society that has practised crisis response and has a long tradition of total defence. The weakness lies in the fact that most civilian infrastructure is privately owned and responsibility is spread across a large number of authorities. It is exactly in those seams that hybrid threats find their way in.

The future: the cognitive battlefield

Generative AI now makes it possible to produce convincing deepfakes in real time. A fabricated surrender order or a fake statement can have immediate political consequences. Cognitive warfare is about shaping how people perceive reality, not just what they believe.

Autonomous systems can compress decision cycles further still. Drones are becoming a standard grey-zone tool: cheap, deniable, and hard to counter without risking escalation. Whoever can act faster than their opponent's decision-making process gains an advantage that does not require firing a single shot.

A lasting condition

Hybrid warfare is not a prelude to war. It is a way of doing politics by other means, in the space between peace and war. For Sweden and Europe, that means security policy has to be built for a "new normal" in which the pressure is



deliberate, events are ambiguous by design, and resilience depends as much on the fabric of society as on military systems.

It is a form of conflict that is not always visible and is not always provable — but it shapes the strategic reality all the same, and it is not going away

/Staffan Scherloff