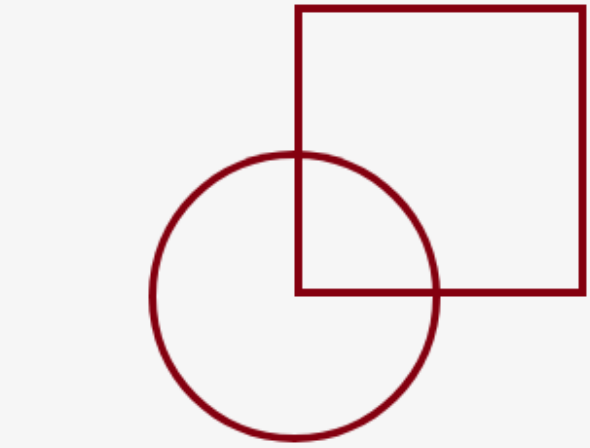
LA LIGNE FINE PAPERS N°4



Hybrid warfare: winning without crossing the threshold of war

Series: Strategic Foundations

Authors: Alek UMONT
Published Date: July 31, 2026

Angle

Hybrid warfare is generally presented as the combination of military, cyber, informational, economic and clandestine means. This definition describes its instruments, but lacks its deep logic.

Hybrid warfare is first and foremost a threshold strategy. It aims to produce political effects comparable to those of an open conflict without offering the adversary the triggering event that would justify a military response, a collective mobilization or the activation of an alliance. Its strength therefore lies not only in the diversity of the means used, but in the methodical exploitation of the institutional, legal and political hesitations of the target.

The challenge is not simply to detect more attacks. It is to build a capacity to respond against actions, each of which seems insufficient to provoke a strong reaction, but the accumulation of which gradually modifies the balance of power.

Executive Summary

Hybrid warfare is neither an entirely new form of conflict nor a sufficiently precise category to refer to any hostile action between peace and war. The combined use of propaganda, subversion, sabotage, economic coercion, irregular forces and clandestine operations has long been part of strategic practice. Contemporary displacement is due to three transformations.

The first is the expansion of attack surfaces. The digitization of societies, the dependence on private infrastructure, the interconnection of energy, financial and information networks and the exposure of democratic processes make it possible to act on a state without directly confronting its armed forces.

The second is the difficulty of attribution. The use of intermediaries, criminal groups, private companies, relay media, cyberattackers or supposedly autonomous actors makes it possible to dissociate the action from its sponsor and to slow down the political decision.

The third is the fragmentation of the response. Hybrid means cross the administrative boundaries between internal security, defence, intelligence, the economy, diplomacy, justice and communication. The attacker coordinates a unique campaign; the targeted state often treats it as a succession of separate incidents.

Hybrid warfare is therefore not necessarily about defeating an army. It seeks to prevent a political system from transforming a diffuse aggression into a collective decision. Its main terrain is not so much the territorial border as the institutional capacity of a state to interpret, attribute and sanction a hostile action.

The answer cannot be exclusively military. It requires a doctrine to aggregate incidents, strengthen the resilience of critical functions, attribute attacks with a degree of politically actionable evidence, and impose cumulative costs on their perpetrators.

Introduction

The success of the expression "hybrid war" is due to its ability to name a reality that has become immediately perceptible: states no longer confront each other solely by diplomacy or armed force. They simultaneously use disinformation, cyber-attacks, sabotage, economic coercion, clandestine operations, instrumentalised migratory pressures, irregular forces and, in some cases, the limited use of military means.

NATO defines hybrid threats as the combination of military and non-military, overt and clandestine means, which can include disinformation, cyber-attacks, economic pressure, irregular armed groups and conventional forces. It also points out that these means are designed to blur the distinction between war and peace, sow doubt and destabilize the targeted societies[1].

This definition is useful, but it risks transforming hybridity into a simple inventory. However, a war is not hybrid because it uses several instruments. Any serious strategy combines political, economic, military and informational resources. Hybridity becomes strategically significant when this combination is organized to exploit the adversary's reaction thresholds.

The aggressor does not always try to remain invisible. Above all, he seeks to remain insufficiently attributable, insufficiently violent or insufficiently spectacular to trigger a response proportionate to the cumulative effect of his actions.

Sabotage of infrastructure, a manipulation campaign, cyber intrusion, the financing of a radical movement or economic pressure can be treated separately as technical, criminal or diplomatic problems. Coordinated over time, these acts can weaken public confidence, disrupt decision-making, increase the cost of a policy and reduce a state's freedom of action. The real power of hybrid warfare lies in this gap: the strategic effect is greater than the political visibility of each of the operations that make it up.

I. The real issue is not the mix of resources, but the control of the threshold

Hybrid warfare is often described as an intermediate conflict in a "grey area" between peace and war. This formulation is intuitive, but it maintains a misunderstanding: it leads us to believe that peace and war are two clearly delimited spaces, separated by an uncertain zone. In reality, uncertainty is not only a characteristic of the environment. It is produced by the attacking actor. A hybrid campaign is designed to make four essential elements questionable: the identity of the perpetrator, the nature of the action, its seriousness and the legally or politically legitimate response.

The difficulty of attribution allows the sponsor to deny his involvement. The ambiguity about the nature of the action makes it possible to present it as an accident, a private initiative, a social protest, a criminal operation or a spontaneous reaction. The apparent limitation of damage prevents each incident from warranting a major response. Finally, legal uncertainty divides decision-makers on the instruments to be used. Hybrid warfare is thus a war against qualification. It is less about preventing the target from seeing that he or she is under pressure than about preventing him or her from agreeing on what that pressure means. However, a

[1] North Atlantic Treaty Organization. (2026, January 29). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

state does not react only to material facts. He reacts to the political and legal qualification he manages to give them.

This strategy is particularly effective against democratic regimes and multinational alliances. They must produce evidence, build consensus, follow procedures and publicly justify their decisions. Their caution is a legal and political strength, but it can become a vulnerability when the adversary organizes its operations precisely to slow down these mechanisms. The attacker then benefits from an asymmetry of decision. A centralized authority can quickly combine means of intelligence, economic coercion, influence, and sabotage. The target, on the other hand, must circulate information between several administrations, compare sometimes divergent analyses and reach the level of evidence necessary for a reaction.

Mastery of the threshold does not mean that the aggressor refuses any escalation. It allows him to choose the rhythm of the dance. He moves forward in limited acts, observes the reaction, adjusts his means and consolidates the gains obtained. The target is faced with a succession of accomplished facts, none of which seems, in isolation, to justify the cost of a confrontation.

II. Hybridity transforms civilian vulnerabilities into strategic depth

Conventional warfare typically seeks to destroy the adversary's forces, infrastructure, and command capabilities. Hybrid warfare broadens the target: it treats the ordinary functioning of society as an operational space. Energy grids, submarine cables, ports, satellites, banking systems, digital platforms, supply chains, electoral processes and the media are no longer just the environment for conflict. They can become its instruments and objectives.

This evolution is not only the result of an offensive doctrine. It stems from the very structure of contemporary societies. Digitalization increases economic efficiency, but it creates systemic dependencies. The outsourcing of critical functions to private companies complicates the organization of their protection. The interconnection of networks allows a local disturbance to produce chain effects. The speed at which information circulates finally makes it possible to immediately exploit any incident politically. A hybrid operation does not necessarily need to cause a hardware collapse. It may have a more limited but politically profitable consequence: to cast doubt on the reliability of an institution, to temporarily disrupt an activity, to cause an increase in costs, to polarize the interpretation of a crisis, or to demonstrate that the state does not have complete control over its territory.

The real target is therefore not always the infrastructure under attack. It can be collective confidence in the ability of the authorities to protect it. A network outage becomes strategically significant when it feeds the idea of a powerless state. A data leak becomes a political instrument when it is selected, contextualized, and disseminated to divide a coalition. A cyberattack produces a hybrid effect when it is articulated with an informational campaign intended to amplify its psychological impact. This is why the distinction between physical attack, cyber operation and information manipulation becomes insufficient. The desired effect results from their articulation. The European institutions now adopt a broad conception of the hybrid threat, including information manipulation, cyberattacks, the use of the law for hostile purposes, economic coercion and the instrumentalisation of migration[2].

However, this extension carries a conceptual risk. If all external pressure becomes hybrid, the notion ceases to help distinguish phenomena. The decisive criterion must remain the

[2] European External Action Service. (2026, March 19). *EU action on countering hybrid threats*. https://www.eeas.europa.eu/eeas/eu-action-countering-hybrid-threats_en

intentional coordination of several actions aimed at systemic vulnerability and an identifiable political effect. Hybrid warfare is not defined by the presence of a particular tool, but by the strategic coherence that links the tools together.

III. The main objective of disinformation is not to convince, but to disorganize

The manipulation of information is often presented as a battle of narratives: an actor would disseminate a false version of the facts in order to make a population adhere to his reading. This dimension exists, but it is not always the central objective.

An informational campaign can succeed without imposing a single belief. Sometimes it is enough to make any information questionable, to exhaust attention, to multiply incompatible interpretations or to persuade citizens that no source deserves special trust. The objective is then not conviction, but disorientation.

This strategy is suitable for information-saturated societies. Scarcity is no longer that of content, but that of attention and the ability to prioritize. The hostile actor does not need to construct a perfectly coherent narrative. It can simultaneously broadcast several contradictory narratives, as long as they converge towards the same result: weakening the possibility of a common interpretation.

Interior polarization thus becomes a multiplier. External information only produces lasting effects if it encounters pre-existing fractures: mistrust of institutions, territorial inequalities, identity conflicts, feelings of downgrading or competition between political memories.

Hybrid warfare exploits more than it creates these divisions. But by amplifying them, it increases the cost of public decision-making. Any response to the hostile actor is then reinterpreted as a partisan maneuver, a restriction of freedoms or an attempt at concealment.

Modern information operations also benefit from inexpensive infrastructures: automated accounts, networks of sites, influencers, synthetic content, targeted advertising and seemingly independent relays. The European External Action Service considers foreign information manipulation and interference as a security threat and has developed a specific methodology to map the infrastructure, techniques and behaviours associated with these campaigns[3]. However, the answer cannot be reduced to the removal of content.

A policy exclusively focused on the false risk of ignoring the strategic function of the campaign. The particular content is often interchangeable. What matters is the distribution network, coordination, targeting and the desired effect. Information resilience therefore implies less the creation of an official truth than the maintenance of institutions capable of establishing the facts, recognizing their uncertainties and communicating quickly without sacrificing their credibility.

[3] European External Action Service. (2025, March 19). *3rd EEAS report on Foreign Information Manipulation and Interference (FIMI) threats: Exposing the architecture of FIMI operations*. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

IV. Attribution has become a power function

A hybrid action is effective when it imposes a cost without clearly exposing the perpetrator to a penalty. Attribution is therefore the point of transition between technical knowledge and strategic decision-making. In the cyber field, the clues are often fragmentary. Digital infrastructure can be leased or compromised. A criminal group may act on its own behalf, with the tacit consent of a State or on the direct instructions of a service. The tools used can be copied or deliberately imitated to direct suspicion towards another actor.

The same problem exists in physical operations. Saboteurs can be recruited through intermediaries, paid through opaque circuits and not know the real sponsor. Private companies, militant groups, or criminal organizations can provide the state with additional distance. Absolute allocation is therefore rarely possible within the time limits required by the decision.

But to demand judicial certainty before any reaction is to offer the aggressor a structural advantage. Conversely, publicly attributing an attack based on insufficient evidence exposes the target to costly error and loss of credibility. Power therefore lies in the ability to transform a body of information into a defensible political judgment.

This capability requires technical means, human intelligence, cooperation with private companies, information sharing between allies and a procedure that allows several levels of certainty to be distinguished.

Attribution must also be dissociated from the full publication of evidence. A State can be convinced of the identity of a perpetrator without being able to set out the sources on which that conviction is based. He must then choose between preserving his intelligence capabilities and convincing his partners or his public opinion.

This dilemma explains the importance of collective attributions. When a group of states arrives at a common assessment, it increases the political credibility of the prosecution and reduces the possibility for the author to divide the responses.

But the attribution is only valid if it leads to a consequence. Naming without sanctioning can help normalize hostile action. Public disclosure must be articulated with a range of responses: legal proceedings, expulsions, financial sanctions, diplomatic restrictions, cyber countermeasures, enhanced protection of infrastructure or exposure of the networks used. Attribution is not only an operation of knowledge. It is an instrument of deterrence.

V. Alliances are strong against a major attack, but vulnerable to the accumulation of incidents

Conventional military alliances are organized around a relatively identifiable event: an armed assault on a member. Their credibility rests on the certainty that this event will produce a collective response. Hybrid warfare attacks precisely this certainty.

Unclaimed sabotage, limited cyber operation, destabilization campaign, or pressure from non-military actors immediately raises several questions: Is the perpetrator a state? Does the action reach the threshold of an armed attack? Is it serious enough to justify a collective reaction? Which instrument should be used?

The more different perceptions of the threat are among the members of an alliance, the more exploitable this ambiguity becomes. The aggressor may target states that it deems politically isolated, economically dependent or institutionally fragile. It can also vary the instruments according to national vulnerabilities in order to prevent the emergence of a common diagnosis.

The goal is not necessarily to cause the collapse of the alliance. It can be more modest: to demonstrate that its guarantees are difficult to activate in the face of limited aggression.

NATO says hybrid action could, depending on the circumstances, lead the North Atlantic Council to invoke Article 5. This possibility maintains a useful deterrent ambiguity, but it does

not solve the political difficulty of aggregating dispersed acts into a campaign serious enough to warrant a collective response[4].
The European Union, for its part, has developed a "hybrid toolbox" including preventive, cooperative, restrictive and supportive measures, as well as rapid reaction teams that can be deployed at the request of a Member State or partner.
These instruments mark an important evolution: the hybrid response is no longer solely a matter of national defence. It becomes an object of institutional solidarity.
However, there is still weakness in the pace of decision-making. A hybrid campaign can evolve on a daily basis, while collective responses require consultations, shared evidence, and compromises between governments.
Deterrence must therefore be prepared before the crisis. Allies must define in advance the categories of actions they wish to address collectively, the mechanisms for accelerated consultation and the responses that can be mobilized without having to rebuild a consensus for each incident.

VI. Hybrid warfare exploits the fragmentation of the state more than it circumvents its military might

Faced with a hybrid campaign, each administration tends to perceive the part of the problem corresponding to its competences. The police are investigating sabotage. The intelligence services are looking for a mastermind. The cybersecurity authority deals with an intrusion. The Ministry of the Economy is analysing commercial pressure. The regulator monitors the platforms. Diplomacy consults partners. The armies observe the associated military activities. Each can do the right thing while missing out on the overall campaign.

This fragmentation is one of the main advantages of the attacker. The latter may coordinate its instruments around a single policy objective, while the target divides them among distinct administrative categories. The first imperative of the response is therefore analytical: to connect the incidents.

This requires a permanent mechanism for merging intelligence, capable of cross-referencing weak signals, identifying regularities and distinguishing a fortuitous accumulation from a coordinated campaign.

The second imperative is political: to designate an authority capable of arbitrating between administrations and making an overall assessment at the governmental level.

The third is operational: having a range of responses that does not necessarily reproduce the means used by the adversary. A cyberattack does not always have to be met with a cyber response. Sabotage can be punished economically. An informational operation can lead to exposure of networks, prosecutions or diplomatic measures.

The most effective response is the one that strikes at the vulnerability of the sponsor, not the one that imitates his instrument. However, this approach presupposes a doctrine. Without doctrine, the authorities oscillate between two excesses: minimizing each incident for fear of escalation or over-characterizing any hostile action at the risk of trivializing the notion of war.

VII. Resilience is essential, but it is not a sufficient strategy

Resilience has become the watchword of Western policies against hybrid threats. It refers to a company's ability to prevent a disruption, absorb its effects, maintain its essential functions and quickly return to normal functioning. This approach is justified.

[4] North Atlantic Treaty Organization. (2026, January 29). *Countering hybrid threats*. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats

A less vulnerable company reduces the return on adverse trades. Redundant infrastructure, trained administrations, prepared companies and a well-informed population limit the possibilities for coercion.

NATO now sees national and collective resilience as a component of deterrence and defence. The European Union has also strengthened its crisis preparedness policies by integrating hybrid risks into exercises, joint assessments and cooperation between civilian, military and private operators[5]. But resilience must not become a doctrine of passivity.

Absorbing attacks indefinitely without increasing the cost to the perpetrator can encourage their recurrence. A repaired infrastructure, a contained disinformation campaign, or a neutralized cyberattack does not mean that the adversarial strategy has failed. This can be aimed at usury, the accumulation of expenses and the trivialization of a permanent state of insecurity. Resilience must therefore be combined with deterrence.

It is not a question of promising an automatic response to each incident, but of building a predictable relationship between the repetition of hostile acts and the gradual increase in the costs imposed. This deterrence must be cumulative, as is the hybrid campaign itself. An isolated action can call for a discreet response. A coordinated set must lead to a change in scale: sanctions, technological restrictions, dismantling of networks, legal actions, reduction of dependencies or targeted countermeasures. The target must demonstrate that he or she knows how to add up incidents where the aggressor is counting on their separate treatment.

[5] European Commission. (2025, March 26). *Preparedness*. https://commission.europa.eu/topics/preparedness_en

VIII. Limitations and objection: the notion of hybrid warfare can obscure more than it illuminates

The concept has several weaknesses. The first is its excessive extension. Cybercrime, disinformation, election interference, economic espionage, sabotage, terrorism, clandestine operations and commercial pressures are sometimes grouped together under the same category. A notion that designates any hostile action ends up no longer prioritizing any threat.

The second is the risk of militarization of public debate. Describing a campaign as a "war" can lead to treating protest, the circulation of false information or economic interactions according to a disproportionate security logic.

The third is the risk of systematic outsourcing. Foreign actors exploit real fractures, but do not always invent them. Attributing any polarization to external interference would avoid the scrutiny of internal political and social responsibilities.

The fourth is reciprocity. The means associated with hybrid warfare are not reserved for authoritarian powers. Democracies also employ sanctions, influence operations, clandestine intelligence, economic pressure and cyber actions. The relevant distinction cannot therefore be based solely on the identity of the actor or on the nature of the tool.

It must relate to the objective, the coordination, the degree of clandestinity and the desire to compromise the political autonomy of another State.

Finally, hybridity does not replace conventional warfare. It can prepare for a military intervention, accompany it or prolong its effects. The presence of hybrid tactics does not mean that armies lose their importance. On the contrary, the credible threat of a conventional force can enhance the effectiveness of pressures below the threshold.

Hybrid warfare is therefore not a new era in which conflicts have become exclusively invisible. Rather, it describes a way of conducting competition in which non-military instruments are integrated into a strategy supported, in the last instance, by a balance of power.

Recommendations

The first priority is to replace the logic of the incident with a campaign logic. States must create permanent mechanisms to bring together cyber, economic, informational, clandestine and physical actions when they appear to meet a common intention.

The second priority is to define cumulative thresholds. The reaction cannot depend solely on the seriousness of each act taken separately. A coordinated repetition must be able to justify a stronger response, even in the absence of a spectacular single event.

The third priority is allocation. It is necessary to develop common procedures between allies, based on several levels of certainty and allowing for rapid political attribution without requiring the publication of all available information.

The fourth priority is the protection of critical infrastructure. This protection must involve the State, local authorities, private operators and foreign partners. It involves redundant networks, securing supply chains, regular exercises, and reporting obligations.

The fifth priority is to make the response multidimensional. The response instrument must not be mechanically identical to the attack instrument. Hybrid deterrence requires the ability to combine judicial, diplomatic, economic, financial, cyber and, where the threshold requires, military measures.

The sixth priority is to protect the information space without creating a ministry of truth. The state must strengthen transparency, speed of communication, access to reliable data, and the ability of researchers, media, and platforms to identify coordinated operations.

Finally, alliances must organize solidarity against aggression below the threshold in advance. Ambiguity can contribute to deterrence, but absolute ambiguity benefits the attacker. Automatic consultations, joint teams and a pre-determined range of responses would help to reduce the time between award and action.

Strategic implications

Hybrid war reveals less the disappearance of war than the transformation of the conditions under which an actor can impose his will. Military power remains indispensable, but it does not automatically protect against political manipulation, economic coercion, cyber attacks, or sabotage of civilian infrastructure. A state can have high-performance militaries while remaining vulnerable if its institutions fail to connect signals, produce credible attribution, and mount a coherent response.

The main asymmetry is therefore not between military and civilian means. It opposes the coordination of the aggressor to the fragmentation of the target. Hybrid warfare thrives when the attacked state seeks a decisive act while the adversary pursues a cumulative strategy. It wins when institutions debate each incident separately and lose sight of the political direction that connects them.

The strategic response must reverse this logic: absorb shocks, reduce vulnerabilities, aggregate hostile actions and impose progressive costs before their accumulation silently transforms the balance of power.

Conclusion

Hybrid warfare is no less real because it often avoids direct military confrontation. It is a strategy designed to achieve political effects while preventing the target from acknowledging in time that he or she is engaged in a conflict.

Its effectiveness is based on a contradiction specific to contemporary states. They are powerful in their different areas of competence, but often weak in their ability to articulate them. They have intelligence services, armed forces, regulators, magistrates, diplomats and competent technical operators. However, they struggle to convert these expert opinions into a common interpretation when the aggression crosses all their categories.

The real issue is therefore not to know where peace ends and war begins. The hybrid adversary builds its strategy precisely on the impossibility of establishing this border with certainty. The decisive question lies elsewhere: can a state recognize a hostile campaign before a spectacular act makes it indisputable?

If he waits for definitive proof, the aggressor retains the initiative. If he reacts to each incident as an open war, he risks one-upmanship and exhaustion. The relevant response is to construct a doctrine of cumulative proportion: tolerating uncertainty about each act without losing sight of the coherence of the whole.

Hybrid warfare is not won by removing all vulnerability. It is neutralized when a company demonstrates that it knows how to transform the ambiguities of the adversary into predictable, coordinated and sustainable costs.