FONDATION ROBERT SCHUMAN

POLICY PAPER

Schuman Paper
n°819
27th January 2026

Jean MAFART

Hybrid threats: from geopolitics to internal security

Although the concept of hybrid threats is now widely accepted despite its rather vague nature, there remains a blind spot in European discussions and strategic thinking: the phenomenon is still rarely addressed from the perspective of internal security policy.

It has long been recognised that hybrid threats – whether cyberattacks, arson, disinformation, interference in electoral processes or the exploitation of migration flows – can strike within our borders. The European Union acknowledged this: the Justice and Home Affairs (JHA) committees regularly address the issue and the Commission gives it considerable attention in its internal security strategy of April 2025. In fact, it is mainly on the basis of hybrid threats that the document justifies the proposal to double the staff of Europol. However, the emergence of these threats in the internal security policies of the EU and its Member States raises important questions, both in terms of principles and operations, most of which remain unanswered.

It is instructive to browse through the wealth of analytical and policy papers available on hybrid threats: the geopolitical dimension of the phenomenon still predominates, and while authors sometimes address the resilience of European states and societies, there is almost nothing to be found on how to respond to these threats in the context of internal security policy or on the necessary adaptation of the instruments of this policy. In other words, it is as if the concept of hybrid threats, which originally concerned defence and foreign policy circles, had forcefully found its way into European internal security policy and had not yet been fully assimilated into the internal sphere. If we add to this the fact that European internal security policy itself remains little known despite the considerable proportions it has taken on in recent decades, the current state of strategic thinking is not conducive to the consolidation of a strategy to deal with hybrid threats in their internal dimension.

However, a strategy of this kind would be very useful, following the example of what has long existed within NATO and the Common Security and Defence Policy (CSDP) for the external dimension: does the issue of hybrid threats, now referred to in every context but without a coherent approach, risk leading European internal security policy astray, diverting it from its primary purpose ? and how can the competences of the Union, its Member States and other actors be harmoniously combined when hybrid threats blur the line between internal and external security, or even between national security – which is in principle the remit of the Member States – and the competences of the Union?

WHAT IS A HYBRID THREAT?

To understand how hybrid threats have emerged in the sphere of internal security, we need to look at the origins of the concept. The Hybrid Centre of Excellence, a research organisation supported by the European Union and NATO, provides a definition: "*Hybrid threats are harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. Such means include* *information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid threats describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare*."

It was through the concept of "hybrid warfare", presented here as the ultimate stage of the "hybrid threat", that "hybridity" entered military and strategic debates in the United States in 2005; this concept "*reflects the porosity between regular and irregular warfare*". In this sense, "hybrid warfare" covers a combination of military and non-military means, which some authors point out is nothing new from a historical perspective: the Peloponnesian War would be a typical example. Even before it entered the internal security debate in another form, Elie Tenenbaum highlighted the gradual dilution of the concept of "hybrid warfare", particularly in light of Russia's invasion of Crimea in 2014: "*Generally unfamiliar with the debates surrounding the concept of hybrid warfare before 2014, European security specialists have taken up the term, but most often to refer to the informational, diplomatic, economic or even energy dimensions of Russian strategy*". It is only a short step from a "hybrid war" conceived in this way to a "hybrid threat": "*Economic warfare, digital propaganda and diplomatic activism have thus also become hybrid threats*." The author is harsh in his assessment of the reasons behind such fervour: "*Hybrid warfare has become a matter of bureaucratic survival for many partners (NATO centres of excellence, think tanks, etc.), who sometimes choose to alter the meaning of the concept to better match their areas of expertise*."

In any case, two key points deserve attention: firstly, hybrid warfare and hybrid threats are geopolitical concepts that originated in military and strategic think tanks; secondly, the extraordinary popularity of the concept of hybrid threats in this field of thought – even before it was taken up by internal security circles – has led to a weakening of the original concept, to the point where its relevance is now challenged. Moreover, another confusing aspect of the hybrid threat is that, while it is similar to war on the one hand, it is also similar to a perfectly acceptable form of peaceful action: there is a growing porosity between hybrid actions and what constitutes influence policy, whether implemented by diplomatic services, the media, research organisations or "pseudo-NGOs". Some authors even classify Chinese investments in infrastructure and research abroad as hybrid modes of action. Alongside clandestine actions – which are just as traditional, incidentally –, new modes of action are developing, which appear more or less innocuous, multiplying the possibilities for foreign interference and making them less identifiable. Moreover, ambiguity is one of the very principles of hybrid action: its perpetrators "*use [...] a range of conventional and unconventional methods (or "tools") that allow them to exploit the vulnerabilities of the target and create ambiguity about the origin (or "attribution") of the attack*"; they thus seek, "*even when facing an adversary who has the upper hand*", to "*reduce the risk of a military response*".

Hybrid threats are by nature external in origin and are treated as such in the relevant defence forums. In its Strategic Concept, NATO clearly states – as a response to the ambiguity of the methods used – that "*hybrid operations against Allies could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty*". Recent drone incursions into the airspace of some European states are a striking example of such operations and the response they can provoke in the military sphere; but we can now deduce from NATO doctrine that a collective response by its members is not inconceivable – at least in principle and beyond a certain threshold of severity – in the face of a combination of hybrid actions that could be more insidious, such as sabotage, cyberattacks or large-scale interference in an election campaign. The European Union, too, has had to acknowledge the hybrid threat in its Strategic Compass.

THE IMPLICATIONS OF HYBRID THREATS FOR INTERNAL SECURITY

Although originating from outside, hybrid threats affect security and stability within Member States and societies. In the digital sphere, the European Network and Information Security Agency (ENISA) presents a rather worrying observation: "*As geopolitical and economic tensions grow, cyber warfare escalates with espionage, sabotage, and disinformation campaigns becoming key tools for nations to manipulate events and secure a strategic advantage*." The 2024 Romanian presidential election is a spectacular illustration of this: while the pro-Russian candidate had come out ahead in the first round, the Constitutional Court annulled the entire election. In the meantime, the Romanian authorities revealed a vast campaign on TikTok, coordinated and financed from abroad, in support of this candidate, who was unknown to Romanians just a few weeks earlier. In March 2025, the Constitutional Court rejected the candidate's application to stand in the new presidential election, sparking unrest in the country.

Taking all modes of action into account, a study shows that the number of hybrid attacks by Russia in Europe almost quadrupled between 2023 and 2024 . The methods used have become very varied, ranging from assassinations to psychological warfare and arson. The study states: "*40 arson plots have been linked to Russia in Germany and Poland* [between 1 January 2018 and 30 June 2025]*, including the destruction of the Warsaw shopping centre. In May 2024, a major fire broke out in Berlin at a Diehl Group factory, which produces IRIS-T surface-to-air missiles used in Ukraine. Russia has also been linked to an explosion at a warehouse in Spain storing communications equipment for Ukraine*."

The use of migration flows is another particularly cynical tactic: the aim is to weaken the EU's external border, but also to undermine confidence in its institutions and sow division. According to the European Commission, irregular flows of people from Belarus increased by 66% in 2024; the Commission mentions that "*Russian authorities are facilitating these movements, given that more than 90% of migrants illegally crossing the Polish-Belarusian border have a Russian student or tourist visa*".

Another striking phenomenon is the use of "subcontractors", often (in Russia's case) Eastern European nationals; the mass expulsions of Russian agents under diplomatic cover following the invasion of Ukraine have probably contributed to the development of this practice. But the latest annual report by Europol on organised crime analyses a more worrying phenomenon, the use of criminal organisations: "*Geopolitical tensions have created a window for hybrid threat actors to exploit criminal networks as tools of interference, while rapid technological advancements – especially in artificial intelligence (AI) – are reshaping how crime is organised, executed, and concealed. These shifts are making organised crime more dangerous, posing an unprecedented challenge to security across the EU and its Member States*." This is how two Iranians were arrested in 2024 after having recruited criminals (involved in drug trafficking) to organise violent actions in France and Germany against Israelis or Israeli interests.

It should be added that hybrid action and organised crime do not only converge in their methods of operation: their objectives are also increasingly similar. Our geopolitical adversaries and criminal organisations, some of which now feel strong enough to attack state institutions – a trend seen in the Netherlands and Belgium but now emerging in France – have the same interest in destabilising the institutions. The collusion between them, which is probably a structural phenomenon, therefore goes far beyond simple "outsourcing".

From an internal security perspective, the concept of hybrid threats is therefore relevant to describe risks to the security of people and property – including the destabilisation of institutions and public services – within the European Union but initiated by hostile foreign powers. Thus the current geopolitical configuration presents a twofold phenomenon: on the one hand, the growing prevalence of these external attacks in the spectrum of threats to internal security; on the other, the increasing convergence of methods and objectives between hybrid action and organised crime.

INTEGRATING THE RESPONSE TO HYBRID THREATS INTO THE UNION'S INTERNAL POLICIES

Effective treatment of hybrid threats, a phenomenon that originates externally but can affect the economy, infrastructure or democratic institutions within our borders, first requires a rapprochement between both external and internal policies: this means being able to mobilise the latter – primarily internal security policy – as part of a comprehensive approach. From this point of view, the concept of hybrid threats is useful both politically and practically: it can help to overcome the inevitable divisions between different public policies. The aim is therefore to take a comprehensive approach to systematically address the vulnerabilities of the European Union and its Member States in all areas of action that may be affected by hybrid actions, without any blind spots.

This integration has been a gradual process. In its conclusions of June 2015 – shortly after the invasion of Crimea – the European Council called for greater effectiveness of the CSDP and pointed "*the need for mobilising EU instruments to help counter hybrid threats*". In other words, hybrid threats are still addressed from an external perspective (the CSDP), but the aim is to use all European policies to deal with them. Subsequently, the Strategic Compass was a milestone in the consideration of hybrid threats; it provides for a set of instruments designed to facilitate coordinated campaigns by Member States in the face of aggression. In 2022, conclusions on hybrid threats set out more detailed guidelines.

With regard to internal security policy, the Council conclusions of 18 May 2015 emphasised "*the need to further strengthen the links between external and internal security*" in order to develop "*further synergies between CSDP, in both its civilian and military dimensions, and Freedom, Security and Justice actors, notably the EU agencies (Europol, FRONTEX and CEPOL)*". The "Joint Framework" published by the Commission in 2016 is the result of these political guidelines. Among other measures, it includes the establishment within the intelligence centre (INTCEN) of a "fusion cell" which "*will receive, analyse and share classified and open-source information*", efforts to monitor and protect critical infrastructure and the design of a "operational protocol" allowing the Union and its Member States to respond in a coordinated manner to a hybrid attack[1].

A 2018 communication specifies the action. But it fell to the Finnish Presidency of the Council – for easily understandable geopolitical reasons – to mobilise the Home Affairs Ministers in order to strengthen the Union and its agencies' efforts to better detect and combat these new threats. Under this presidency, in 2019, the Council set up a permanent working group on hybrid threats. The conclusions of December 2019 reaffirm two principles: firstly, "*the primary responsibility for countering hybrid threats lies with the Member States*" (as part of their national security missions), with the European Union's action being complementary; secondly, a "*comprehensive approach to security*" must involve all actors, national and European, civilian and military, public and private.

Quite logically – but to a spectacular extent – the 2025 internal security strategy devotes considerable space to the subject, with eight pages out of thirty. The document confirms the "cross-cutting" approach to hybrid threats: one chapter presents instruments developed and discussed in various forums, far removed from those specialising in hybrid threats.

The theme of "resilience of critical entities" is an excellent example of this approach. A directive of 14 December 2022 requires Member States to adopt a national resilience strategy and to carry out a risk assessment at least every four years. These "critical entities" are varied (energy, transport, banking sector); they are themselves required to carry out a risk assessment, take preventive measures, and organise controls and exercises. A regulation deals with the "digital operational resilience of the financial sector". This system involves many European and national administrations, well beyond Home Affairs ministries, and a multitude of private actors.

[1] The European Union Intelligence and Situation Center (INTCEN), attached to the European External Action Service (EEAS), is mainly fed by contributions from the intelligence services of the Member States.

Following the 2020 cybersecurity strategy, the NIS 2 directive (meaning "networks and information security") was adopted in 2022. While the NIS 1 Directive applied to seven sectors, such as health, energy, banking and water suppliers, the new directive covers public administrations, waste management and the space sector. In addition, as requested by the Council, in February 2024 the Commission presented a revision of the 2017 action plan, which organises the joint response to cybersecurity crises. Adopted on 6 June 2025, this revision was approved by the ministers responsible for telecommunications (rather than those responsible for internal affairs).

Finally, we should mention internet regulation: here again, addressing hybrid threats requires the mobilisation of numerous public and private actors, well beyond the traditional circles of security policy. The Digital Services Act (DSA) of 19 October 2022, for example, requires major search engines and internet platforms (those with more than 45 million active users in the EU) to implement risk mitigation measures, particularly with regard to generative artificial intelligence: this is one of several ways of preventing foreign interference in electoral processes. Moreover, the protection of democratic institutions has almost become a European policy in its own right: the "European Democracy Action Plan" of December 2020 has led to several texts, for example regarding the financing of European political parties. On 12 November 2025, the Commission published its "democracy shield", designed to better combat hybrid threats to democracy, including online disinformation. It is very telling that this future "shield" had been announced in the internal security strategy.

A popular geopolitical concept in vogue and initially linked to foreign and defence policy, the hybrid threat has now become widely incorporated into the European Union's internal policies. Achieving this required a two-pronged process: a convergence between external and internal policies, and one between these internal policies, so that internal security issues could be fully taken into account. In this second process, the concept of hybrid threats essentially plays a role comparable to that played by terrorism since the 9/11 attacks: in both cases, there is a need to recognise that the threat has taken on various dimensions and that it must be addressed in all relevant internal policies. Whereas counter-terrorism was once the preserve of the police and intelligence services, it now involves the control of banking flows, digital technology and even firearms. The same dynamic is now at work in the field of hybrid threats.

European internal security policy still needs to achieve with hybrid threats what it has achieved with terrorism: to go beyond concepts and strategies and establish a genuine operational organisation.

ORGANISING A "EUROPEAN CONCERT" WITHIN THE FRAMEWORK OF THE EUROPEAN INTERNAL SECURITY POLICY

The distinctive feature of European internal security policy, more so than trade policy for example, is that it constantly intertwines the competences of the Union and those of its Member States. This is even more true in the case of hybrid threats, since they largely fall within the scope of national security tasks that the European treaties entrust solely to the Member States[2]. It is therefore with good reason that the 2016 Joint Framework granted to the latter primary responsibility for combating hybrid threats. However, two key factors threaten this balance: on the one hand, the worsening geopolitical situation has led the European Union – starting with the Commission – to take sometimes spectacular initiatives in the field of national security and even defence (which some Member States, notably Germany, have been quick to criticise); on the other hand, the very broad, even vague, nature of the concept of hybrid threats lends itself to confusion between the Union's sphere of responsibility and that of the Member States.

This presents an initial challenge: how to organise a genuine "European concert" on hybrid threats, with the EU competent in many areas, the Member States and a multitude of private actors, all in close connection with the CSDP? In this context, the first issue to be addressed is the European Union's capacity for anticipation or, to put it more accurately,

[2] It is in the name of this national security competence that, for example, the Europol Regulation of 8 June 2022 does not authorise the agency to enter notifications concerning suspects into the Schengen Information System (SIS) on the basis of information from third countries: Member States strongly opposed this proposal from the Commission. This was still a matter of terrorism and not counter-espionage, which is an essential task in the fight against hybrid threats but falls within the realm of state sovereignty.

intelligence. We have already heard a variety of proposals on this sensitive subject, reflecting not only the diversity of viewpoints but also, perhaps, a certain amount of uncertainty.

A useful framework for reflection is the "preparedness" and "readiness" strategy undertaken by the European Union following the "Niinistö Report" of October 2024. While the report and the European work it inspired focus on preparedness for all forms of crisis, they obviously devote considerable attention to hybrid threats. However, the report does not merely recommend greater efficiency in the exchange and use of intelligence, which it rightly identifies as a major aspect of crisis preparedness: it proposes to "*develop a proposal together with Member States on the modalities of a fully-fledged intelligence cooperation service at the EU level […] without emulating the tasks of Member States' national intelligence organisations*". This cautious foray into intelligence, which is the preserve of Member States, highlights a delicate aspect of the problem: by blurring the distinction between internal and external security, hybrid threats blur the line between the competences of the Union and those of the Member States even more than before. Moreover, the Niinistö report proposes the creation of an "anti-sabotage" network: the relationship between the EU and its Member States is just as sensitive in this area, since it concerns intelligence and even counter-espionage.

Thus, the "European Strategy for a Union of Preparedness" published in March 2025 suggests that the European Union should have its own information and anticipation capacity and a "EU crisis coordination hub" within the Commission. The simplest solution would be to strengthen the Single Intelligence Analysis Capacity (SIAC), which is part of the European External Action Service (EEAS) and includes INTCEN. At least, that is what the "preparedness" strategy proposes. Similarly, the internal security strategy "urges" Member States to "*enhance intelligence sharing with SIAC*" and "*ensure better information sharing with EU agencies and bodies*".

Rather than European integration of intelligence functions, which has no chance of happening in the foreseeable future, it is therefore once again the concept of networking or cooperation that should be promoted. Moreover, the intelligence community has long been organised outside the framework of European institutions and agencies, but in close cooperation with them. From this point of view, the principles set out in the 2016 "Joint Framework" remain entirely relevant: "*Insofar as countering hybrid threats relates to national security and defence and the maintenance of law and order, the primary responsibility lies with Member States, as most national vulnerabilities are country-specific. However, many EU Member States face common threats, which can also target cross-border networks or infrastructures. Such threats can be addressed more effectively with a coordinated response at EU level by using EU policies and instruments […].*"

Therefore, one could be surprised to hear the recent announcement of the creation of a Commission-specific intelligence service, at least according to the *Financial Times* last November, which has been condemned by several MEPs. In reality, this Commission initiative appears to focus more on internal security; it should be viewed in conjunction with the creation of a "Security College", which aims to keep Commissioners better informed about the level of threats, and a general trend towards strengthening security procedures. However, combating hybrid threats requires improved security within European institutions. Accustomed to transparency and democratic procedures, these institutions have long been negligent in addressing the risk of espionage and interference, which is exacerbated by hybrid threats. That is why, in cooperation with Member States and the European intelligence community, efforts have been made in recent years. These have resulted, for example, in the Regulation of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. However, from the point of view of both prevention and repression of espionage and interference, the European institutions are largely dependent on the police and intelligence services of the Member States, starting with those in Belgium; it is therefore also the responsibility of the Member States to finally provide the Union's institutions with an adequate protection framework.

A second challenge to be addressed is that of the European agencies, particularly Europol: not only has the Commission called for its staff to be doubled and for it to be made a "truly operational police agency", but it has justified this on the grounds of the need to give it more resources to deal with hybrid threats. The internal security strategy states that "*the Agency's current mandate does not cover new security threats such as sabotage, hybrid threats or information manipulation.*" The Commission is referring here to resources (human and operational) and legal means. Given the lukewarm reception by most Member States, these weakly substantiated proposals are unlikely to be implemented in their entirety. The Member States' perplexity is not only due to the lack of any reasoned assessment of staffing needs: it is also a question of policy.

The first point of policy concerns the nature of Europol: its "mandate" (Regulation of 11 May 2016) makes it an agency dedicated to "*preventing and combating serious crime*", intended to support the police services of the Member States, and which is not designed to deal with the phenomenon of hybrid threats as a whole. While it is probably wrong to make "intelligence" strictly speaking an exclusive competence of Member States – the judicial police themselves engage in "pre-judicial" intelligence activities –, the primary purpose of Europol and the police forces of Member States is to deal with hybrid threats within a criminal justice framework. From this point of view, hybrid action does not exist as such: it can take the form of sabotage, arson, intrusion into a computer system or even assassination. This is also the meaning of recent comments by Executive Director Catherine De Bolle: "*Hybrid warfare itself is not part of Europol's mandate. However, we address the criminal activities that intersect with hybrid tactics, such as cyberattacks, disinformation used for fraud or extortion, and the misuse of AI. Europol works closely with Member States and other EU bodies to share intelligence and strengthen Europe's resilience*."

A second point of policy relates to the sensitive issue of "attribution". Publicly naming the perpetrator of a hybrid attack is an operational and political choice that falls within the realm of national security and foreign policy. This public attribution by the targeted State may appear to be a necessary form of response: publicly naming an aggressor is the only way to dispel the ambiguity inherent in hybrid modes of action and, in some cases, to justify countermeasures or sanctions. This was the choice made by France last April, when the Minister of Foreign Affairs identified the Russian GRU as the perpetrator of cyberattacks against "*a dozen French entities since 2021*". A clear policy of attribution is even "essential to deterrence". Conversely, circumstances may render such an attribution inappropriate. This sovereign choice obviously belongs solely to the States, and it is understandable that they do not want a European agency designed as an instrument to combat hybrid threats as such.

While it is therefore illusory to see Europol as the European Union's armed wing in the fight against hybrid threats overall, it should be noted that judicial action – and the involvement of law enforcement in general – is certainly set to develop: the response to hybrid threats cannot be conceived solely from the point of view of resilience and prevention, which have been the focus of most European efforts over the last ten years. The growing collaboration between "hybrid actors" and criminal organisations, as well as the increasing convergence of their objectives and modes of action, further justifies this judicial effort. In this perspective, the development of the agency's human and technical resources undoubtedly responds to an operational need (which still needs detailed assessment), and the possibility of supplementing the Europol Regulation in force with regard to the categories of offences that determine the agency's scope of competence should not be ruled out. It is also interesting to note that the Ministers for Home Affairs, meeting on 8 December 2025, announced their intention to "*provide law enforcement agencies with the necessary capabilities*" to deal with drones.

These developments in the role of the police in combating hybrid threats tie in with an interesting aspect of the Niniistö report. The report does not only consider hybrid threats as a threat to internal security: it also addresses the contribution of internal security policy in the face of hybrid threats. The issue of access to digital data for investigative services, for example, has been a pressing problem for criminal investigation and intelligence services in specialist forums for several years, but it now appears to be a key issue for European resilience. In line with the conclusions of the "high-level group" on data access, set up in June 2023 by the Council and the Commission, the report recommends, in particular, to "*to ensure the creation of a robust framework for lawful access to encrypted data to support the fight of Member States' authorities against espionage, sabotage and terrorism, as well as organised crime*". The internal security strategy takes up these guidelines.

Similarly, the role of Frontex should be clarified: just as much as the fight against irregular immigration, the fight against hybrid threats justifies strengthening the Union's external border and increasing surveillance of its periphery. In September 2025, the proposal to build an "anti-drone wall" caused quite a stir, but the Commission's reflections on the threat posed by drones go back further: a 2023 communication already provided a fairly detailed analysis and proposals, in particular on the joint development (between the Union and the Member States) of "anti-drone solutions". More recently, the Commission has mobilised significant funding in this area and plans to set up a "centre of excellence" within its research centre in Ispra, Italy (over which a drone — probably Russian — flew in March 2025). The question of drones, which was on the agenda of the JHA Council meeting on 8 December 2025, sparks sensitive discussions within the EU about the role of Frontex.

The Commission wishes to propose legislative changes that would allow the agency to strengthen its action against drones: like the agency itself, it is calling for Frontex to have access to all data relating to threats (in particular those from the SIAC) and to cooperate closely with the armed forces and intelligence services of the Member States. There is also talk of strengthening the agency's operational capabilities against aerial and maritime drones. However, Member States will be very careful to ensure that Frontex is not turned into an agency to combat hybrid threats on the border. The current discussions are representative of the uncertainties surrounding the division of roles between the EU and its Member States regarding this phenomenon – hybrid threats in general and drones in particular – that challenges the traditional *summa divisio* between European competences and national security missions. Here again, the solution probably lies in the notion of "concert", i.e. the ability of actors to work in a network to prevent structural or *ad hoc* overlaps in competences, which are inevitable, from degenerating into conflicts of competence.

From this pragmatic perspective, the European Union suffers from at least two weaknesses. The first is the lack of an overall vision of the phenomenon of hybrid threats and of political impetus in the area of internal security: the dual process at work – bringing together the external and internal dimensions on the one hand, and internal policies on the other – remains incomplete. Admittedly, the Commission does have this overall vision, as demonstrated by its internal security strategy: even more so than the previous strategy (2020), this document reflects a commendable effort to take all hybrid threats into account in European internal security policy. It includes the revision of the Cybersecurity Act of 17 April 2019, just presented on 20 January 2026, a plan on port security (to strengthen the security of port infrastructure and supply chains), a new action plan on CBRN (chemical, biological, radiological and nuclear) risks, and work specifically on the instrumentalisation of migration flows (a subject on which the Commission published a communication in December 2024). By deciding to subject all legislative initiatives to a prior impact assessment in terms of security and "preparedness", the Commission has taken a step forward in taking a comprehensive view of the phenomenon, beyond the usual actors in internal security policy. Furthermore, there is political momentum among heads of state and government, as evidenced by the progress made in the Union's various internal policies. In its conclusions of December 2024, the European Council proclaimed that "*the European Union and the Member States will continue to strengthen their resilience and make full use of all means available to prevent, deter and respond to Russia's hybrid activities*". Finally, the JHA Council frequently addresses the issue of hybrid threats and, in December 2024, the ministers of Justice and Home Affairs adopted "strategic guidelines" that give them their rightful place (while noting that "*the principle that national security remains the sole responsibility of each Member State is to be explicitly taken into account*"). It was also in this spirit that the action plan on submarine cables was presented to the ministers for Home Affairs in March 2025.

However, the European response to hybrid threats can only be fully integrated into internal security policy if ministers for home affairs have been given primary responsibility for it at the domestic level: a powerful driving and coordinating force is required, with an overview of the threat but also of the progress made in all areas. This is where the dual nature of the Council can be valuable: as the ministers for Home Affairs are responsible for all aspects of European internal security policy — even though texts on cybersecurity, digital issues or the resilience of the financial sector are discussed in other Council configurations — and responsible for national security in their Member States, it is up to them to discuss a comprehensive strategy and ensure that the threat is properly taken into account in all the Union's internal policies. Just as they have been meeting as the "Schengen Council" since 2022, one could imagine the JHA Council adopting a specific work programme on the internal dimension of hybrid threats and periodically reviewing its progress. One could also imagine the Council appointing a coordinator for hybrid threats, just as it did in 2004 when it appointed a coordinator for counter-terrorism: the aim is not to build a cumbersome institutional structure, but to ensure that security objectives are considered and that there is the necessary fluidity between the various European policies concerned.

The second weakness stems from the fact that the overlap of competences between the Union and its Member States is bound to increase and, for the time being, there is no effective mechanism to deal with potential conflicts of competence. The agencies' management boards, which deal with strategic issues and major priorities, are not the appropriate forum: there is undoubtedly a need to devise flexible arrangements for direct consultation between the many European and national actors who are called upon daily, in one capacity or another, to deal with hybrid threats to internal security. One of the tasks of a European coordinator could be to initiate discussions on such a framework for consultation.

Finally, an effective policy to combat hybrid threats, given the multitude of actors that they are likely to affect, requires that public authorities succeed in fully involving businesses – starting with "operators of vital importance", which are subject to increasingly stringent European legislation. Economic actors are aware of this, as shown by the proliferation of initiatives taken by large companies to protect themselves from cyber-attacks, espionage, reputation damage and physical damage. A "culture of security" is emerging, along with a culture of "resilience" and "crisis management". As security departments are strengthened (at least for companies that can afford it), a set of processes and methods must gradually be imposed on senior management and all business divisions. However, they cannot accomplish this task alone: beyond raising awareness among economic actors about industrial data protection, for example, public authorities must be able to set out a clear vision of the threats, disseminate a prevention policy and, where necessary, organise close operational cooperation between public and private actors (either to deal with a crisis when it arises or as part of jointly organised crisis exercises). Protecting our economic potential and infrastructure is not just a matter for European legislation; it also requires greater investment by the Union and its Member States in their relations with economic actors.

***

The issue of hybrid threats poses formidable challenges for European internal security policy: historically designed to respond to internal issues – initially to offset the effects of free movement between Member States –, the European Union's internal security policy must adapt its instruments to a phenomenon that is imposed on it from outside but affects Europeans and their institutions at the very heart of the continent. Beyond the coordination efforts between the domains of the CSDP and the JHA, we must prepare to face a threat whose scale, but above all whose nature, is unprecedented. Many questions remain unanswered, and empiricism will undoubtedly play a considerable part in this effort to adapt; but it is still necessary to clearly identify the problems and vulnerabilities that need to be addressed.

Jean Mafart

Prefect, former Director of European and International Affairs at the Ministry of the Interior, author of "Politique européenne de sécurité intérieure" (Bruylant, 2025), Member of the Scientific Committee of the Robert Schuman Foundation

You can read all of our publications on our site:
www.robert-schuman.eu/en

Publishing Director: Pascale JOANNIN
ISSN 2402-614X

The opinions expressed in this text are the sole responsibility of the author.

THE FONDATION ROBERT SCHUMAN, created in 1991 and acknowledged by State decree in 1992, is the main French research centre on Europe. It develops research on the European Union and its policies and promotes the content of these in France , Europe and abroad. It encourages, enriches and stimulates European debate thanks to its research, publications and the organisation of conferences. The Foundation is presided over by Mr. Jean-Dominique Giuliani.