FONDATION ROBERT SCHUMAN

POLICY PAPER

Schuman Paper
n°787
15th April 2025

Jean MAFART

Hybrid threats, new horizons for the internal security of Europe?

Even today, most of our fellow citizens are unaware that the European Union is actively involved in the fight against terrorism, money laundering and drug trafficking, in border protection and in the harmonisation of criminal legislation[1]. This is why a European internal security strategy, ProtectEU published by the Commission on April 1st is important : it defines the European Union's work programme for the coming years, within the framework of the guidelines laid down by the European Council. The assessment of the previous internal security strategy (for the period 2020-2025) shows that this kind of programme has real scope: the Commission announced numerous initiatives that were actually completed, even if, as time goes by, the action inevitably deviates from the initial intentions in response to circumstances.

Since the successive strategies are work programmes for a given period, none of them really resembles the previous one. On the other hand, the major underlying themes vary relatively little: terrorism, organised crime and external border control were, as it is the case today, key concerns of the '*founding fathers*' of the '*area of freedom, security and justice*' (AFSJ). The doubling of the staff of Europol, the agency responsible which supports Member States in the fight against crime, and the tripling of the staff of the European Border Guard, which are part of the Frontex agency, are also the most spectacular proposals of the new strategy, even if they had already been voiced by the President of the Commission at the beginning of her second term.

The arrival of a new theme is therefore bound to attract attention: in this case, it is striking to see the space given over to hybrid threats (a whole chapter, eight pages out of the thirty in the document published on 1 April). A sad sign of the times: it is no longer conceivable to develop an internal security policy without addressing, alongside the more 'traditional' themes, the growing threat of destabilisation operations of all kinds coming from Russia or elsewhere. The link between the internal and external dimensions of security is obviously nothing new: in France, the White Paper on defence and national security published in 2008 already considered that '*the distinction between internal and external security is no longer relevant*'. Current geopolitical tensions and the development of hybrid threats are blatantly reinforcing this. How can the 'internal security of Europe', initially conceived to respond to internal issues - compensating for the effects of free movement between Member States - adapt to take better account of threats from the outside?

HYBRID THREATS, A PHENOMENON THAT BLURS THE LINE BETWEEN INTERNAL AND EXTERNAL SECURITY

The notion of the hybrid threat is still relatively recent in official language. In France, the Revue stratégique 2022 defines 'hybrid strategies' as '*deliberately ambiguous combinations of direct and indirect, military and non-military, legal and non-legal courses of action, often difficult to attribute*', which '*can have significant consequences for democracies because they aim to delegitimise them, weaken their moral forces*

[1] J. Mafart, « L'"Europe de la sécurité intérieure", méconnue, mérite intérêt et moyens », Libre Belgique, 6 March 2025.

and cohesion, or reduce their economic and national defence potential'.

Hybrid threats are therefore by nature of external origin and treated as such in defence-related bodies. In its Strategic Concept, NATO also clearly states 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*'. The European Union has also had to take note of the hybrid threat in its Strategic Compass, which sets out its priorities in terms of security and defence: '*State and non-state actors are using hybrid strategies, cyberattacks, disinformation campaigns, direct interference in our elections and political processes, economic coercion and the instrumentalisation of irregular migration flows. […] Our competitors are not shying away from using emerging and disruptive technologies to take strategic advantages and to increase the effectiveness of their hybrid campaigns.*'

These various threats, which come from outside, nevertheless affect security and stability within the Member States and societies themselves. Cyber-attacks are the most obvious example, whether they involve sabotage (to neutralise the information system of a public administration or a large network company, for example), electronic espionage or the manipulation of electoral processes. In its most recent annual report the European Agency for Cybersecurity (ENISA) makes a somewhat disconcerting 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*.'

Confirming this serious threat, the Romanian presidential election in December 2024 gave rise to an unprecedented decision: although the pro-Russian far-right candidate had come out ahead in the first round, the Constitutional Court annulled the entire election. In the meantime, the Romanian authorities had uncovered a vast campaign on TikTok, coordinated and financed from abroad, in support of this candidate who was unknown to Romanians a few weeks earlier. In March 2025, the Romanian Constitutional Court's decision to reject the candidate's application caused unrest in the country: the initial goal of the '*hybrid operation*' had probably not been achieved, since Mr Georgescu will not be President of the Republic, but such unrest is in itself a very significant result for its designers, as the episode will have contributed to undermining citizens' confidence in democratic institutions.

The exploitation of migratory flows, a particularly cynical mode of action, follows the same logic: the immediate objective is to weaken the external border of the European Union, but it also aims to undermine confidence in the institutions and create divisions. In a communication dated December 11th, the Commission indicates that, in 2024, irregular flows from Belarus increased by 66%. It specifies 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*'.

The most recent annual report by Europol on organised crime ('SOCTA') highlights another phenomenon: the direct use of criminal networks by our adversaries. '*Serious and organised crime is in the grip of a profound transformation. 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 alliance between hybrid warfare and organised crime can be seen in many areas, including computer sabotage, digital data capture, social media campaigns using fake accounts and arms trafficking. It is a mutually beneficial type of cooperation: the states involved have an additional mode of action, enabling them to conceal their involvement, while the criminal organizations benefit in terms of revenue, protection from prosecution and even access to new technological resources.

GREATER EUROPEAN INVOLVEMENT IN ALL FIELDS

The Strategic Compass marked a milestone in the recognition of hybrid threats; in particular, it provides for

the creation of a '*hybrid toolbox*', a set of instruments designed to facilitate coordinated campaigns by Member States in the face of aggression. Following this, the conclusions of the Council on hybrid threats developed more detailed guidelines. However, the European Union did not wait for the Strategic Compass, let alone the new internal security strategy, to include hybrid threats in its policies. Hybrid threats are like terrorism or organised crime: many EU initiatives contribute to their prevention, even if they have a broader purpose.

The cyber security policy is a very good example of this. The 2020 cybersecurity strategy published jointly by the Commission and the European External Action Service (EEAS). Gave notably rise to the NIS2 directive dated December 14th 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 even the space sector. The European Union has also set up a '*joint cyber security unit*' which provides rapid response teams and develops a policy for the prevention of cyber-attacks with public institutions and companies. Furthermore, as invited to do so by the European Council in its conclusions of 22 May 2024, last February the Commission presented a revision of the 2017 action plan which organises the joint response of the EU and its Member States to cyber security crises.

Note should also be taken of a second directive dated 14 December 2022: it relates to the resilience of critical entities. Member States are now required to adopt a national resilience strategy and to carry out a risk assessment at least every four years. These 'critical entities' – whether in the energy, transport or banking sectors – are themselves required to carry out risk assessments, take preventive measures and organise checks and exercises. A third text of 14 December 2022 completes this arsenal: the regulation on digital operational resilience in the financial sector, or DORA regulation. Furthermore, Russia's actions in the Baltic Sea are not foreign to the action plan published in February 2025 to protect submarine cables.

The protection of democratic institutions, meanwhile, has given rise to a veritable profusion of initiatives that have an obvious internal purpose – the rule of law is unfortunately under threat within the Union itself – but are also aimed at responding to interference from abroad. The 'action plan for European democracy' of December 2020 led to several important texts such as the regulation of 13 March 2024, which strengthens the rules on the financing of European political parties. On 26 April 2024, the Commission published '*guidelines on recommended measures to mitigate systemic risks online that may impact the integrity of elections*': intended for the main search engines and Internet platforms (those with more than 45 million active users in the Union), this document published in application of the Digital Services Act (DSA) of 19 October 2022 imposes risk mitigation measures on the companies concerned, for example with regard to generative artificial intelligence. In December 2023, the Commission also presented a proposal for a directive intended to regulate activities involving the representation of interests on behalf of third countries. Finally, we await the forthcoming publication of the '*Democracy Shield*', designed to better combat hybrid threats to democracy, particularly online disinformation. It is revealing that this future 'Shield' is mentioned in the 2025 internal security strategy: once again confirmation is given that our internal security cannot be conceived without taking into account threats of external origin.

As for the instrumentalisation of migratory flows, the '*crisis situations*' regulation of 14 May 2024 provides an initial response: this allows for the management of massive flows at the external border, in particular by derogating from the normal rules for examining asylum applications. At the same time, the construction of fences by certain Member States cannot be ignored: 13% of the external border (which represents a total length of 12,000 km) would now be fenced off[2]. Although the European Commission has always refused to finance such infrastructure, significant budgetary resources have been mobilised at the request of the European Council to improve the security of the external border, particularly through technological detection equipment (radar, cameras, drones, etc.).

Hybrid threats are multifaceted, so it is not surprising that the European Union's response is too. But hybrid threats also evolve rapidly, forcing the European Union

[2] An assessment of the state of the EU Schengen area and its external borders – A merited trust model to uphold Schengen legitimacy, *European Parliament, May 2023.*

constantly to adapt; the effort made in recent years can therefore only be a first step. The new internal security strategy provides an overview: among the many measures to come, there is, for example, the forthcoming revision of the Cybersecurity Act, a regulation of 17 April 2019 that sets out the tasks of ENISA and defines the European cybersecurity certification framework, a strategy for ports (to strengthen the security of port infrastructure as well as supply chains), a new action plan on CBRN (chemical, biological, radiological and nuclear) risk and work specifically on the instrumentalisation of migratory flows (a subject on which the Commission already published a communication in December 2024).

WHAT ADJUSTMENTS SHOULD BE MADE TO INTERNAL SECURITY POLICY?

The developments devoted to hybrid threats in the strategy published on 1 April reflect full recognition of the increasing overlap between internal and external security. However, two distinct public policies, involving different actors, remain. Of course, the European Union has long been working to prevent them from being completely cut off from each other: in its recent conclusions, for example, the Council looks at the effective coordination of the EU's internal and external policies on terrorism and violent extremism. In this area, as in others, the 'justice and home affairs' (JHA) and common security and defence policy (CSDP) forums sometimes hold joint meetings. Similarly, the action plan on submarine cables was presented to the interior ministers at the JHA Council last March.

However, the development of hybrid threats calls for deeper questioning: in this respect, the new strategy must be brought closer to other European work. In September 2024, Ursula von der Leyen announced a '*dynamic preparedness*' strategy as part of a comprehensive approach to crises. The following month the report by former Finnish President Niinistö on preparedness and readiness to crises, on which the current work is based, was published. It is striking to note that, in parallel with the growing presence of hybrid threats in internal security policy, the latter is also considered an essential element in the fight against hybrid threats. This brings us back to the issue of borders: Sauli Niinistö considers it essential to '*ensure effective control of the Union's external borders through all available means*'. Similarly, the issue of access to digital data for investigative services, a criminal investigation and intelligence problem that has been very prevalent in 'JHA' forums for several years, appears in the report as a challenge 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 '*ensure the creation of a robust framework for lawful access to encrypted data […] to support the fight of Member States' law enforcement and security authorities against espionage, sabotage and terrorism, as well as organised crime*'. The 1 April strategy takes up these guidelines.

It is therefore quite natural that we come to the issue of intelligence. According to Article 4 of the Treaty on European Union (TEU), '*national security remains the sole responsibility of each Member State*'. This guarantees the competence of the Member States in matters of intelligence. That is why, in the Europol regulation of 8 June 2022, the Council firmly opposed the agency being authorised to enter alerts concerning suspects (particularly in relation to terrorism) in the Schengen Information System (SIS) based on information from third countries. In practice, however, the distinction between national security and the competences of the Union has become more blurred, either as a result of European case law – the CJEU's Tele 2 judgment, in particular, called into question the possibility for Member States to oblige telephone and Internet operators to retain their subscribers' connection data for the purposes of any investigations that may be carried out[3] – or by the will of the Member States themselves. One example among many: even though it also has a judicial purpose, the PNR Directive of 27 April 2016 – adopted at the insistent request of the Council – organises a system for the collection and processing of data for purely administrative purposes of prevention, i.e. for intelligence purposes[4]. However, the report does not limit itself to recommending greater efficiency in the exchange and exploitation of intelligence, which it rightly considers a major aspect of crisis preparedness: it proposes to '*develop a proposal together with Member States on the modalities of a fully-fledged intelligenced cooperation*

[3] *'While the effectiveness of the fight against serious crime […] may depend to a large extent on the use of modern investigative techniques, such an objective of general interest, however fundamental it may be, cannot alone justify a national regulation providing for the generalised and indiscriminate retention of all traffic and location data being considered necessary for the purposes of the said fight'; CJEU, 21 December 2016, Tele 2 Sverige, § 103. – In France, the case law of the Council of State allowed for the retention of an operational system for the use of connection data; CE, 21 April 2021, no. 393099, Quadrature du Net.*

[4] *PNR data is what travellers provide at the time of booking, particularly when purchasing a plane ticket (identity, address, date of travel, payment method, full itinerary, etc.). Combined with API data (the data provided at the time of check-in), they enable a large-scale risk analysis approach to detect passengers who correspond to predefined 'risk profiles' (particularly with regard to terrorism or drug trafficking). PNR data can also be compared with European or national police files for the purposes of searching for persons or for judicial investigations.*

service at the EU level […] without emulating the tasks of Member States' national intelligence organisations'. Aware that he is venturing into minefield, Sauli Niinistö is extremely cautious in his language. However, this proposal highlights a fundamental aspect: by weakening the distinction between internal and external security, hybrid threats also blur the boundary between the competences of the Union and those of its Member States, even more than before. Moreover, the Niinistö report also proposes the creation of an 'anti-sabotage' network: once again, the relationship between the Union and its Member States is delicate since we are in the realm of intelligence and even counterespionage.

From a 'sovereigntist' perspective, these various developments could lead to fears of further encroachment on the powers of the Member States. This would be rather futile: the weakness – and the paradox – of a purely 'sovereigntist' approach is that the more European developments are perceived as exogenous and detrimental to the prerogatives of States, the more one tends to feel powerless due to a lack of understanding of how the extraordinarily powerful vehicle of the European Union, despite its slowness, can be used to promote effective policies. The value of the current discussions on the '*Europe of internal security*' and its relationship with external threats is that they invite us to organise a true European concert. The Member States are solely responsible to their people for their most important asset, security; it cannot be otherwise, even if the Commission sometimes gives the impression of having an ulterior motive (why double or triple the staff of an agency before even assessing the needs?).

The contribution of the Union and its agencies in the field of security has become decisive, including in areas such as terrorism, where some Member States intended to remain in sole control some fifteen years ago. All have learnt a great deal from the crises of the past decade, whether they be migratory waves, terrorist attacks or COVID: it is now proven that they can organise themselves in a flexible and responsive manner to deal with crises at European level. Hybrid threats undoubtedly call for a similar level of organisation and networking, with due regard for each party's area of expertise. The European Union's work on crisis preparedness will therefore be decisive: one of the key challenges is to bring together stakeholders and public policies that are still too separate. In this sense, the new European internal security strategy is far more far-reaching than the measures it contains.

Jean Mafart

Prefect, former Director of European and International Affairs at the Ministry of the Interior, author of the Politique européenne de sécurité intérieure (Bruylant, to be published)

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

Publishing Director: Pascale JOANNIN
ISSN 2402-614X