

Jacek M. Raubo

HYBRID THREATS TO POLAND AND FRANCE



Introduction

Firstly, it should be emphasized that the concept of "hybrid warfare" is unfortunately highly misleading. A definitional approach pointing to hybrid activities or the conduct of hybrid warfare is suggested instead. In this case, hybrid activities are a kind of synergy between the influence of classic state structures (secret services, military, etc.) and other elements that are usually intended to camouflage the existence of a state entity in the background of events. At the same time, however, it is not possible to make a clear distinction between peacetime and wartime, which is particularly important from the point of view of the attacked state or states. The latter cannot simply implement legal tools such as a state of war, nor can they carry out pre-emptive and, above all, offensive actions, as is the case in a classic armed confrontation. Currently, hybrid actions can be observed particularly in the space below the threshold of war, but there is a risk that a potential adversary may also use them to prepare a more classic form of aggression. It should be noted that in terms of tools, hybrid actions can cover almost all domains, referring, for example, to provoking or strengthening illegal migration channels, exploiting organized crime, conducting or provoking terrorist activities, and resorting to mercenary groups or private military companies (PMCs). Furthermore, one should also take into account more state-like activities, such as secret operations by special services, diversionary and sabotage activities, as well as intensified operations in the information and cognitive domains (especially through the use of PSYWAR/PSYOPS). It should be noted that for some time now, the activity of special services around the world has reached levels previously seen only during the Cold War, and may even have surpassed them in certain respects. This refers to an increased willingness to spy on each other using a variety of tools – HUMINT, SIGINT, IMINT, MASINT, , as well as the development of OSINT. This encourages attempts at risky forms of activity and acceptance of potential crises. This can be seen, for example, in the murders of dissidents, opposition figures, and other personal targets.

Hybrid Threats to Poland and France

Importantly, weapons of mass destruction, specifically a radioactive agent and a powerful chemical substance (Novichok), were to be used on the territory of a European country (primarily the United Kingdom). Since 2014 (dating back to, for example, the explosion at the ammunition depots in Vrbětice, Czech Republic), diversionary and sabotage activities have also become visible, which are now reaching an ever-increasing scale and posing greater threats to the safety of bystanders. At the same time, massive operations are being carried out in the information and cyber spheres, the scale of which is also likely to be similar to that of the Cold War period or even exceed the standards of that time. Therefore, it should not be forgotten that modern hybrid activities may also relate to elements closely linked to technological development. In the cyber domain, there are activities of so-called "patriotic hackers," but also concentrated and often long-term actions by APT groups. Operations using electronic warfare (EW) means are also becoming visible.

Finally, attention should also be paid to the development of unmanned technologies, which enable a rapid expansion of possible scenarios for various forms of hybrid activities. In this case, we can talk about kinetic strikes using unmanned aerial, sea, and land vehicles. It is also important to emphasize the possibility of harassment using similar means, e.g., through mass violations of airspace in protected areas (critical infrastructure, military bases, logistics facilities, etc.). Finally, there may be increased coordination between the use of unmanned systems and organized crime or terrorist structures. Experience on NATO's eastern flank, but also in the Middle East, shows that when organized crime and the hybrid activities of a given state structure intersect, it is easy to blur the line between strictly criminal and parastatal (including, above all, espionage) activities.

Today, in Europe, each of the countries belonging to the EU and NATO must take into account the possibility of hybrid threats occurring on its territory. The main threat in this regard is, of course, the policy of the modern Russian state. The Kremlin authorities are tied to years of military aggression against Ukraine and are looking for tools to influence European countries. Russia's previous ability to influence the West has disappeared or been severely limited. Firstly, because Russia's energy blackmail (based on oil and gas) has failed. Secondly, because European countries have largely taken on the responsibility of containing Russia, including providing military and non-

Hybrid Threats to Poland and France

military assistance to Ukraine. The current Russian authorities are therefore looking for tools other than typical political-economic or political-military blackmail. That is why they are resorting to hybrid activities with such intensity and are teetering on the brink of war. The strategic goal is to break up Europe and even vassalize a significant part of the continent, referring to the former so-called sphere of influence from the Soviet era. The operational goal is to weaken military and non-military aid to Ukraine, destabilize individual European countries or draw them to their side, or possibly neutralize their attitudes. The tactical goals are to temporarily shift activities, such as diversionary and sabotage, but not only these, to their frontline situation.

However, hybrid threats should not be equated solely with strictly Russian activity. In the case of European countries, such tools may be used by other countries. Chinese influence is becoming increasingly visible in the cyber, information, and cognitive domains. When it comes to migration, organized crime, or the instrumental support/use of terrorism, we are talking about the interests of some countries in the Middle East and even North Africa (as Spain, for example, has often found out). Hybrid actions allow the state invoking them to hide, at least formally, or to attempt to camouflage its involvement. It should be noted that this may refer to both official (diplomatic and political) denial, as well as attempts to shift responsibility onto another state or non-state structures, and to attribute some of the actions to internal factors within the attacked state.

Poland and France in a Similar Strategic Situation

What currently connects Poland and France in terms of hybrid threats is primarily their position in relation to the European security system. Given its size, France is obviously a potential target, as it is one of the world's most important powers, defining policy directions in many areas. It is a country that is active not only in Europe, but also in the Indo-Pacific and Africa. What is more, it is a country with a very assertive defense policy, including deterrence through nuclear weapons. Poland, on a smaller scale, is an important link in the security of NATO's eastern flank and the Baltic Sea region, and thus also in terms of cooperation with the Nordic countries. In both cases, we are talking about state entities involved in the security guarantee system and members of NATO/EU. This automatically gives rise to hybrid actions against them by Russia, but also by other countries interested in destabilizing and weakening the European

Hybrid Threats to Poland and France

security architecture (including in the context of relations with non-European entities). In the latter case, this primarily concerns France, as its policy has been contested, for example, in relation to the Indo-Pacific, the Mediterranean, and African countries. Most importantly, when it comes to hybrid actions, in both cases (Polish and French) we are discussing not so much a forecast of potential threats, but rather actual incidents and crisis situations.

Tools for influencing Poland and France

- actions targeting the political system, primarily in the realm of information. In both countries, attempts at systematic external interference in socio-political debates, particularly in relation to elections, should be noted. Of course, the case of France's defence against threats to the presidential elections is described in more detail in the literature on the subject. However, it is to be expected that further attempts will be made using a system of developing communication tools. This applies to a number of methods, not just the most popular term, i.e., disinformation (or possibly also the simplified term fake news). We must remember that real opponents have the ability to increasingly improve their microtargeting of specific groups of people in society. The aggressor's ability to absorb new and groundbreaking technologies is also increasing, led by the support of tools based on broadly understood Artificial Intelligence (AI). What is more, the Internet is becoming increasingly important for both societies in terms of shaping socio-political attitudes. In addition, the defence system is highly complex, as it involves reflection on the limits of freedom of speech and expression in democratic countries. Aggressors, such as Russia, can exploit any limitations on the part of the democratic system and have no restrictions on using their own PSYOPS/PSYWAR resources in the form of special services and the military. What is more, in their case, there are no restrictions on the use of typically offensive methods. The goals are to cause instability in both countries in terms of socio-political, economic, and even technological issues. In the latter case, it should be noted that nuclear energy is an important issue in both countries, and this may generate attempts at hybrid influence. When it comes to socio-political and economic issues, any activity that allows for radicalization, creates strong polarization, reinforces anti-state trends, and antagonizes international relations (including the system of relations between countries, e.g., within NATO) can become a space for external activity. In this case,

Hybrid Threats to Poland and France

France must take into account the synergy effect, as, in addition to Russia, it must consider other actors wishing to exert hybrid influence on its policy in the Indo-Pacific, the Caucasus, or Africa. Both countries must therefore be capable of assertive and, above all, effective strategic communication. The French side, bearing in mind its experience, e.g., with the development of VIGINUM, should play a leading role in the transformation of information security architecture in Europe. Unfortunately, Poland still faces the challenge of creating information security units on a national scale, primarily within the framework of coherent (as mentioned above) strategic communication. Thus, Polish-French relations after the Treaty of Nancy can be further strengthened based on cooperation in the information domain and, for example, a joint technological approach to responding to such threats.

- actions in the cyber domain. Poland is currently one of the countries most frequently attacked by state actors and those associated with them in the context of cyberspace. France is also significantly exposed to, for example, large APT group campaigns, and with changes in various strategic dimensions in Europe and the Indo-Pacific, this risk is increasing. Therefore, cyber resilience, the ability to respond to cyber incidents, and the observation of current and future cyber challenges should be treated on a par with the threat to the information domain in both countries. Equally important, both countries need to continuously strike a balance between state involvement, which is insufficient on its own, and the activity of private entities, which are critical to cybersecurity. To further outline the complex layout and structure of cybersecurity, it is necessary to mention not only classic threats, but also hardware issues and cybersovereignty. Actors engaging in hybrid activities against Poland and France understand all the complexities very well and, unfortunately, have mapped out certain weaknesses on both sides (e.g., rapid digitization does not always go hand in hand with the proper implementation of good cybersecurity practices). What is more, an aggressor has the ability to make numerous mistakes with virtually no consequences, which cannot be said about the side defending its cyberspace.

- sabotage and diversionary activities, secret operations by special services, and an increase in the scale of classic espionage. For several years, both countries, and above all their counterintelligence services (primarily the DGSI and ABW), have been reporting that Russia, but also other countries, are making various attempts to use

Hybrid Threats to Poland and France

their own special services to the detriment of Poland and France. The first sign is, of course, the increased scale of espionage, especially in view of the Polish-French stance on Ukraine. Foreign intelligence services have targeted programs such as training assistance and material and equipment support for Ukraine. However, now, after 2022, in both cases, we must also speak directly about a number of threats related to covert operations, and not just espionage itself. First and foremost, the threats are attacks or attempted attacks on critical infrastructure and industry (especially the arms industry). It can be noted that many of the diversionary and sabotage activities are intended to be harassing in nature, building psychological pressure and requiring states to take additional protective measures. In France, and currently in Poland, a significant contingent of armed forces is involved in supporting internal security forces. This is important because some diversionary and sabotage activities may be hidden under the simple camouflage of terrorist threats (the line between them is quite blurred and difficult to define). This is particularly true given that some terrorist activities may be carried out under a false flag. What is more, the inspiration may come from a camouflaged state actor who refers to well-known and recognizable terrorist structures (e.g., Al-Qaeda or Daesh). This is facilitated, for example, by Russian reconnaissance of the Middle East and Africa, which is carried out using intelligence resources and mercenaries. What is more, some activities can now be carried out remotely, solely through internet communication. It should be noted that the Russian secret services simplify the recruitment of one-off agents (untrained individuals, often volunteers), for example, by using their knowledge of channels of communication via Telegram, etc., instant messengers/encryptors (E2EE). This is particularly true in the case of France and Poland, where hostile secret services may seek out supporters of radical ideas (recruitment using ideology), but above all by using tools related to financial offers. This increases the risk of both minor acts of sabotage or diversion, but also of terrorist attacks. This is particularly true given that the latter would become a valuable asset in diverting attention from conventional armaments, Russia's activities in Ukraine and towards NATO's eastern flank (from Norway to Romania). This does not change the fact that Operation Sentinelle, as well as, for example, the new Polish Operation Horizon, involve military forces and resources that are, in a sense, taken out of their current tasks. It should be noted here that it is therefore necessary for both countries to promote investment in European cooperation between counterterrorism

Hybrid Threats to Poland and France

services and counterintelligence agencies. This should primarily involve intelligence sharing, but also the exchange of best practices and awareness-raising among the general public. It is also important to develop synergies between police and military activities in response to the growing scale of threats from unmanned systems. It has already been mentioned that critical infrastructure, but also, for example, mass events, can be harassed by unmanned aerial vehicles, and in the future also by unmanned means from other domains. Importantly, both countries are discussing this not so much as a challenge for the future, but as a threat they are facing in real time on an increasing scale. From unmanned aerial vehicles flying over nuclear power facilities in France to the intrusion of decoy drones into Polish airspace.

- actions involving controlled migration to or through both countries. Poland and France are currently highly sensitive to issues related to migration processes. This sensitivity is, of course, in the socio-political sphere, which has implications for security trends. Currently, Poland is feeling the effects of Belarusian-Russian actions to create an artificial channel for the transfer of illegal migrants across the border with Belarus. Since 2021, Poland has been de facto involved in repelling diverse, but always organized and coordinated, actions by Belarusian-Russian services. Their scenarios involve creating media pressure, provoking socio-political tensions, causing border incidents, and creating pressure for a significant deployment of forces and resources to secure the borders. France must take into account other types of threats resulting from the possibility of external radicalization based on migration issues, as well as an increase in the scale of migration across the borders of other countries. Another important factor for France is the issue of security within the English Channel. This is, of course, a consequence of the transfer of illegal immigrants from France to the United Kingdom. The common denominator for both countries is the instrumental use of migration pressure by external actors seeking to weaken both countries and cause tensions within them.

- actions involving organized crime. Both Poland and France must take into account the instrumental use of organized crime in the hybrid activities of other state actors. This applies both to the support of previously signalled threats of espionage, diversion, and sabotage by appropriately infiltrated and recruited criminal groups. However, it may also concern an increase in the scale of drug-related threats, as well as the scale of

Hybrid Threats to Poland and France

violence used by organised and less organised criminal groups. In both countries, consideration should be given, for example, to the possibility of a controlled influx of weapons, ammunition and explosives based on the war in Ukraine, but also from other directions. It should be noted that many external countries have so far used their contacts with organized crime. Such contacts on the Russian side are well known, but other countries in Africa, the Middle East, and even Asia (e.g., the Democratic People's Republic of Korea) should also be taken into account. Combating organized crime is also essential from the perspective of limiting money laundering and any economic and financial irregularities that could affect the security of both countries. This issue is also linked to the fight against terrorist threats.

Conclusion

In summary, hybrid activities targeting Poland and France have many commonalities. This allows for the development of cooperation in the area of diverse security activities between the two countries. The recent Treaty of Nancy (2025) should therefore be seen as an opportunity to gain even greater capacity to exchange best practices, create the necessary platform for intelligence sharing, and synchronize pre-emptive actions through synergies, e.g., the ability to detect sources of threats and anomalies signalling their potential occurrence in the future. Another advantage is the change in the strategic attitude of the French authorities towards the security of NATO's eastern flank countries, including Poland. The limitation, of course, is the fact that France, as a power (describing itself not so much as a regional power as one providing the necessary strategic balance in other regions of the world), has much more scattered global interests. Poland must therefore accept and, in a sense, understand some of them, knowing that even artificially supported illegal migration from Belarus and Russia requires action both at the external borders of the country in Europe and in the Middle East, Africa, the Caucasus, Central Asia, and Africa. This may bring the interests of both countries closer together and, above all, signal common strategic needs. However, the priorities remain combating hostile hybrid activities in the information, cognitive, and cyber domains. It should be remembered that we are talking about challenges that may provide opportunities for cooperation not only at the institutional level (political, military, special services, and police), but also in terms of technological development. This is particularly true given that some of the challenges in the cyber

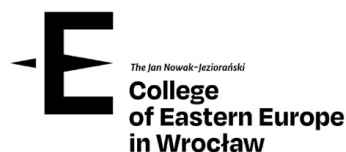
Hybrid Threats to Poland and France

and information-cognitive domains, as well as, for example, physical protection against sabotage, diversion, and terrorism, may require the development of new technological solutions. Thus, we can suggest that, in the case of similar hybrid threats, it is possible to jointly develop or (and) improve specific technologies (which is also important in the area of absorption of EU funds for security and defence within consortia of existing companies, the R&D sector, or the academic sphere).

Jacek M. Raubo is an analyst with Defense24 analyst and lecturer at Adam Mickiewicz University in Poznań.

Public task financed by the Ministry of Foreign Affairs of the Republic of Poland within the grant competition "Public Diplomacy 2024 – 2025 – the European dimension and countering disinformation.

The opinions expressed in this publication are those of the authors and do not reflect the views of the official positions of the Ministry of Foreign Affairs of the Republic of Poland.



November 2025

Edited by Laurynas Vaičiūnas

Proofreading: Niall Gray

DTP: Dolasu

ISBN 978-83-7893-420-2