

The material is part of a publication by the Romanian New Strategy Center "Black Swans in the Black Sea" 2026, Coord. Lt. Gen. Ben Hodges and George Scutaru

THE BLACK SEA SECURITY DILEMMA: ESCALATION RISKS IN A FRAGMENTED STRATEGIC ENVIRONMENT

Yordan Bozhilov, President of the Sofia Security Forum

Russia's war against Ukraine, now in its fourth year, threatens not only Ukraine but the whole Euro-Atlantic security. The Black Sea region is exposed to a wide range of risks and threats which, combined with weak regional cooperation, EU and NATO's shortfalls in the area create possibilities for escalation. The dynamics in the development of the transatlantic relations lead toward greater uncertainty. The Black Sea is no longer a peripheral theatre but a strategic testing ground where hybrid pressure, alliance cohesion, and nuclear deterrence intersect.

The Black Sea region is in the process of profound structural shifts driven by both regional dynamics and external strategic pressures. Historically, in the evolution of the Black Sea region from the end of World War II to the present day, several clearly distinguishable periods can be identified. During the Cold War, the Black Sea represented a heavily militarized zone and a potential arena of military confrontation between the Warsaw Pact and NATO. As on other lines of contact between the two blocs, a high degree of caution prevailed here as well, driven by the danger that any escalation could turn into an armed conflict with the risk of escalation to a nuclear war. It was precisely this strategic deterrence that shaped the behavior of both blocs.

The collapse of the USSR and the Warsaw Pact, as well as the democratic transition of some countries, led to a significant reduction of tensions in the Black Sea region. This period was marked by the development of more friendly relations and intensified regional cooperation. A number of agreements and initiatives were signed, such as BLACKSEAFOR, the Confidence and Security Building Measures in the Black Sea (CSBM), the Border Police Coordination Center in Burgas, and

others, which created a framework for interaction and additional confidence-building mechanisms among all littoral countries.

During this period a number of bilateral disputes were resolved. For example, Bulgaria and Turkey signed a maritime delimitation agreement in 1999, ending a long-standing dispute. The dispute between Ukraine and Romania was settled through the International Court of Justice.

The reduction of tensions in Europe and in the Black Sea created a sense of lasting peace and led to a sharp reduction in military spending and, consequently, to a significant reduction in the military capabilities of most states in the region.

Russia's military actions against Georgia in 2008, the annexation of Crimea and the start of the war in Eastern Ukraine in 2014 fundamentally changed the security environment in the Black Sea. These events led to a dramatic shift in the balance of power, leaving Georgia and Ukraine practically without naval capabilities and redefining regional spheres of influence. Russia gained a strategic advantage and began building a large-scale anti-access/area denial (A2/AD) system.

Russia's confrontational actions were not properly politically interpreted by NATO and the EU. They were perceived as isolated incidents aimed at resolving specific regional or bilateral issues, which resulted mainly in symbolic sanctions and the creation of various negotiation formats. Instead of building adequate military capacity, many political leaders focused on avoiding direct confrontation with Moscow. At the same time, NATO Black Sea states did not take sufficient measures to strengthen their own military capabilities. This miscalculation carries a high price today, as Russia is waging a full-scale war against Ukraine and it is increasingly clear that its objectives are not limited to controlling part or all of Ukrainian territory, but also include territorial expansion and the imposition of spheres of influence.

Without doubt, the Black Sea would have had a very different strategic profile if Ukraine had not managed, through asymmetric actions, innovative tactics, and the use of new technologies, to inflict heavy losses on the Russian Navy and force it to limit its activity. Nevertheless, Russia continues to possess superior naval power, allowing it to threaten other states in the region and create risks for international shipping.

Russia's occupation of Ukrainian land territories and its claims to corresponding internal waters and an expanded exclusive economic zone generate additional sources of conflict, especially as these maritime claims remain unrecognized by Western states.

As a result of Russia's activities strategic confrontation in the Black Sea is re-emerging, but in a qualitatively different form from that of the Cold War. One of the key differences is Russia's retention of significant military potential, including nuclear capabilities, which surpass those of the other Black Sea states.

This raises serious questions related to risk calculation and management in the region, especially given that Russia is a nuclear power with substantial conventional capabilities. If during the Cold War there was parity that guaranteed nuclear deterrence, today we face an aggressive nuclear power with a dominant military presence in the Black Sea.

In this context, a key question is how Russia will use this advantage to achieve its goals in the region and in Europe. Crucial to this calculation is the position of the United States and NATO. Unfortunately, evolving signals and debates in the United States raise questions and create a sense of uncertainty among Alliance members: whether the U.S. would intervene in the event of aggression, whether it would guarantee the nuclear umbrella as the ultimate form of deterrence, and to what extent Article 5 commitments are unconditional.

Even if this uncertainty leads to broader strategic ambiguity within NATO, more problematic is how such signals may be interpreted by Russia. Until recently the full US commitment to European security looked unquestioned, today doubts exist. This ambiguity calls into question the willingness of a number of European member states to act decisively in a potential crisis if they lack US support.

There is a real risk that Russia may perceive this situation as an opportunity for itself. Russia may assume that a certain type of aggressive actions, if limited or below the threshold of open war, or a conflict of limited intensity and territory, would not trigger an adequate and unified response from NATO. Such a development would mean a de facto dysfunction of the Alliance, a result Russia clearly seeks, aiming to divide the United States and Europe, weaken NATO, and undermine the EU.

These considerations apply to Europe as a whole but are particularly relevant to the Black Sea region, where the situation differs significantly from that in the Baltic Sea, for example. In the Baltic region, there is a high degree of political and military unity among the regional countries, as well as constantly strengthening defense cooperation. In the Black Sea, by contrast, interaction between NATO members Bulgaria, Romania, and Turkey remains significantly below both the level of necessity and potential. The only initiative currently implemented by the three NATO countries is the Mine Countermeasures Task Group Black Sea (MCM Black Sea), whose tasks are limited to reconnaissance, exercises, exchange of experience, and the neutralization of drifting naval mines. There are discussions about expanding the mission to include protection of critical infrastructure, but talks are at an early stage.

Against the backdrop of weak regional cooperation, NATO and the EU also face deficits in the region, especially in the maritime domain.

NATO has repeatedly emphasized in its strategic documents the importance of the Black Sea region, but concrete initiatives have not been implemented. A serious issue is also the inability of NATO member states to propose mechanisms for cooperation and Alliance engagement in the years before the war, a question that appears even more complex today, when the Black Sea is part of the war zone. At the same time, Turkey imposed restrictions on the straits connecting the Black Sea with the Mediterranean, preventing NATO ships other than those of Black Sea states from entering the region. NATO has the possibility to increase its presence on the land and in the air, or to use maritime drones, for example, but the shortfalls in the naval domain are serious.

On its part, the European Commission adopted in 2025 document called Strategic Approach to the Black Sea. The document is aimed at building a comprehensive approach focused on strengthening security and resilience and supporting Ukraine. The document clearly defines three main pillars of the approach, being security, stability, and resilience; sustainable growth and prosperity; and environmental protection, climate change resilience, and preparedness. Despite the ambitious agenda, the document lacks an implementation mechanism and no targeted funding has been allocated. Implementation will depend mainly on the initiative and the resources of individual states, primarily EU Black Sea member countries.

Against this background, the Black Sea region is a place where diverse risks and threats are concentrated. The most significant is the ongoing war, but there are others as well refugee flows, drifting naval mines, environmental risks, targeted hostile actions by Russia, illegal arms proliferation, and more, which can be and already are leveraged by Moscow in its interests.

An example of such an approach is the “weaponization of migration.” Through manipulation of public opinion via propaganda and disinformation, in a number of Eastern European countries negative attitudes toward Ukrainian refugees have emerged. The methods and messages in these campaigns are similar and clearly coordinated, resulting in further divisions within European societies.

Drifting naval mines pose a constant risk to shipping and there have already been cases of ships seriously damaged or sunk due to incidents with floating mines. The presence of drifting mines also creates a favorable environment for concealing deliberate sabotage against ships and infrastructure, presented as accidental incidents. As long as the war does not end with a peace agreement, this risk will remain.

Environmental factors can also be used as a tool for economic pressure, including through damage to the tourism sector by spread of false information. Even the mere suggestion of marine pollution can lead to serious economic losses.

These are only some of the possible scenarios and ways in which Russia may use existing risks and threats to its advantage.

Moscow’s strategic interest is to undermine transatlantic relations, erode trust in NATO and attack the values and unity of the EU. In pursuing these goals Russia will use all measures in its arsenal. Until now, these activities were carried out mainly through disinformation, propaganda, and support for certain organizations and media outlets. In recent years, however, there has been a clear expansion and intensification of hybrid actions, including drone incursions into the airspace of NATO and EU states, the disruption of communication cables, intelligence activities, sabotage, assassination attempts and more. In most cases, attribution remained unclear, complicating efforts to prove the direct responsibility of the Russian state.

Whether this trend will continue would largely depend on the resilience, readiness to respond, and ability of NATO and EU states to deliver a unified response.

To illustrate how hybrid escalation could unfold in practice, the following forward-looking hypothetical scenario explores how a combination of cyber disruption, disinformation, and maritime incidents could trigger a cascading regional crisis and test NATO's decision-making and unity.

BLACK SWAN SCENARIO IN THE BLACK SEA

SCENARIO: "THE DEVIL'S EYE"

Phase 1: A Routine Breakdown?

One morning in 2027, residents of Sofia discover they cannot withdraw cash from ATMs, while card payments are widely declined. The reaction is muted as similar problems have occurred before. Banking institutions explain the situation as "temporary technical difficulties with an external provider."

Within the next few hours, several ministry websites become inaccessible, electronic registries stop functioning, and online access to administrative services is disrupted. Society and institutions interpret what is happening as yet another example of inefficiency, outdated IT infrastructure, and poor coordination.

Phase 2: Underestimation and Misattribution

By noon, the disruptions deepen. Problems emerge in mobile networks and delays occur in the operation of the emergency number 112. Internal institutional analyses suggest a combination of DDoS attacks against DNS infrastructure and compromised data flows, but there is insufficient evidence of a targeted state-sponsored attack. The first cautious statement appears, noting that Sofia may be the target of a cyber incident. This does not change public behavior. The lack of an adequate response from the state in previous cases such as cyber-attacks with the leak of personal data of millions of citizens and attacks against banks and companies made people passive because responsibility was not sought. It remained to be seen how the situation would develop.

Phase 3: Escalation of the Problem

During the night, electricity supply in parts of Sofia fails. Telecommunications nodes, data centers, and traffic management systems are affected. Hospitals switch to backup power, but problems arise with fuel supplies for generators and with internal IT systems.

This is the first clear signal that the crisis is systemic rather than an isolated technical failure.

Phase 4: Varna - The Cyber Crisis Intensifies

Almost simultaneously, similar events unfold in Varna. Banking transactions are blocked, electricity supply is interrupted in stages, and mobile networks operate unstably. Urban transport stops due to power outages and failure of control systems.

Conflicting messages appear on social media, fake profiles posing as institutions warn of a new Armageddon. Panic among the population grows.

Phase 5: The Incident at the Port of Varna

At the height of the crisis, the large commercial vessel “Ermita,” carrying hazardous chemical substances for a major industrial facility in the region, enters the Varna port channel.

Due to the system disruptions, the port’s navigation and communication systems operate only partially. Coordination between tugboats, support vessels, and emergency services is compromised. As a result, the ship “Ermita” collides with a small support vessel. A fire breaks out and spreads rapidly. The fire creates a real risk of toxic leakage, large-scale pollution, or an explosion, turning the vessel into a chemical bomb. The population recalls the tragic 1977 incident involving the burning oil tanker “Erma” in the Port of Varna, when the city faced the threat of a devastating explosion that, according to experts, could have destroyed everything within a 2-kilometer radius. Historical memory intensifies the panic.

Phase 6: Collapse of Governance and Public Order

Firefighters, police, and medical services operate with severely limited communications. A common operational picture is lacking.

Water supply and sewage systems begin to experience difficulties due to their dependence on electricity. Queues form at gas stations. Hospitals postpone planned operations. Thousands attempt to leave Varna, blocking exit routes. Incidents occur with a significant number of injured and fatalities.

Phase 7: Geopolitical Revelation

It becomes clear that Bulgaria is the target of a major cyberattack and is attempting to manage the situation but lacks the capacity to repel the attack and perform rapid and reliable attribution on its own. Overnight, partner intelligence services provide information with a high degree of confidence that a structure linked to Russia's Main Intelligence Directorate (GRU) has reportedly launched a coordinated cyber operation against countries in the Black Sea region. The assessment indicates a targeted attack against energy, financial, and maritime systems, combined with disinformation, carried out by Russia.

Russian MFA spokesperson denied any role in the incident calling allegation another example of Russophobia.

Phase 8: Political Dilemma in Sofia

The government convenes an emergency meeting. The Minister of Defense proposes notifying NATO and activating Article 4 consultations. The government is divided. Part of the political leadership fears that such a move would lead to escalation and worsen relations with Moscow. The decision is postponed. Bulgaria loses critical reaction time.

Phase 9: Regional Escalation and Crisis Within the Alliance

Parallel to the situation in Varna, similar scenarios unfold in Constanța. Romania reacts immediately, activates Article 4 and raises the question of invoking Article 5, arguing that the large-scale cyberattacks produce effects comparable to an armed attack across all operational domains: land, sea, air, and cyber.

Phase 10: North Atlantic Council Meeting. Diverging Allied Positions as a Test of Alliance Unity

The North Atlantic Council convenes in an extraordinary session. Discussions are tense and reflect differing strategic cultures and threat perceptions within the Alliance. Some states support a firm response, while others insist on caution due to the lack of “absolute” attribution and fear of direct confrontation with Russia.

The positions of key member states reveal deep internal fractures within the Alliance. Bulgaria hesitates between the need for collective support and fear of escalation, leading to delayed decisions and the loss of strategic time. Romania, facing similar attacks, strongly insists on invoking Article 5, viewing the crisis as a direct attack on the territorial and societal security of the Alliance. Turkey adopts a pragmatic stance, assessing the crisis as a manageable regional problem and expressing the view that Bulgaria, Romania, and Turkey possess sufficient capacity to cope independently even under a scenario involving a severe chemical incident without formally triggering Article 5.

At the same time, the United States is heavily engaged in the Middle East and approaches the situation cautiously, supporting allies with intelligence and logistics but without pushing the Alliance toward immediate collective escalation. The United Kingdom offers concrete assistance, including cyber teams, maritime surveillance, and expert support as a signal of commitment without directly insisting on Article 5. In contrast, some Central European countries openly oppose activating Article 5, citing escalation risks and the need for dialogue. France adopts a politically firm line, emphasizing that NATO must act decisively and unitedly to prevent deterrence from being undermined. The Baltic states and Nordic allies with direct historical and geopolitical experience of Russian behavior strongly support Bulgaria and Romania, insisting that the absence of a clear response will encourage future hybrid attacks against the entire Alliance.

As a result of these differences, no decision is reached to activate the full spectrum of collective mechanisms.

Article 5 and the Cyber Domain: The Threshold of Collective Defense

The crisis raises the fundamental question of applying NATO's Article 5 in the context of a large-scale cyberattack with real physical consequences. Although the Alliance has formally recognized cyberspace as an operational domain and acknowledges that a severe cyberattack could trigger Article 5, in practice there is no clear and commonly accepted threshold for when "cyber" equates to an armed attack. In this scenario, the attacks not only paralyze financial, energy, and communication systems but also lead to a potential incident involving mass casualties and environmental disaster. Nevertheless, difficult and delayed attribution, combined with plausible deniability by the attacker, creates a strategic grey zone in which the political will for a collective response lags behind the actual scale of the damage. Thus, Article 5 becomes not an automatic protection mechanism but a subject of political interpretation, undermining its deterrent effect.

Conclusion: The Black Sea as a Test for the littoral countries, NATO and EU

The presented scenario is hypothetical and aims to draw attention to the Black Sea as a region characterized by multiple risks and threats. It clearly demonstrates the security vulnerabilities of the Black Sea region. Hybrid attacks below the threshold of open war can cause massive damage: economic, social, infrastructural, and environmental without automatically triggering a collective response. The Black Sea offers Russia an opportunity to test the Alliance by undermining trust in it. Delays and political hesitation in decision-making call into question NATO's unity and reliability, turning the Black Sea region into a key zone for provocation and strategic pressure on the entire Euro-Atlantic security system.

At the same time, the scenario underscores the need to develop national crisis-response frameworks for cyber and other type of incidents, which may originate from a variety of actors. Effective protocols are required to ensure coordinated action

between state institutions and private operators, as well as the capacity for rapid attribution and responses.

For NATO, maintaining unity is of critical importance, as it remains a powerful deterrent against a wide range of hostile actions. Given that cyberattacks will continue to pose a significant risk, NATO must invest greater efforts in developing a common policy and coordinated responses. Equally important is the enhancement of regional cooperation for managing and responding to different crisis situations.

The analysis and the hypothetical “Devil’s Eye” scenario demonstrate that the greatest vulnerability in the Black Sea is not only military imbalance, but the intersection of hybrid risks, fragmented regional cooperation, and strategic ambiguity within NATO and the EU. To reduce escalation risks, regional countries must shift from reactive crisis management toward a resilience-by-design approach that integrates cyber defense, maritime safety, and civil protection. Bulgaria, Romania, and Turkey should move beyond ad hoc coordination and institutionalize trilateral operational mechanisms, including a permanent crisis coordination framework, joint maritime domain awareness and expanded missions for existing initiatives such as the Mine Countermeasures Task Group Black Sea toward protection of critical infrastructure and port security. At the national level, governments need to strengthen resilience of energy, telecommunications, financial and other systems, develop clear procedures to act in complex crisis situations and establish rapid attribution and strategic communication capabilities that can prevent panic and counter disinformation during hybrid crises.

For NATO and the European Union, the central challenge is to translate strategic recognition of the Black Sea’s importance into tangible operational and financial commitments. NATO should develop a clearer framework for responding to large-scale hybrid attacks, including clear consultation mechanisms, rapid cyber and intelligence assistance and reaction. Regular cross-domain exercises combining cyber disruption, civil emergency response and maritime incidents would help reduce decision-making delays and strengthen deterrence by demonstrating Alliance cohesion. At the EU level, the Strategic Approach to the Black Sea requires concrete implementation tools, dedicated funding, measurable projects, and coordinated resilience programs. Only through closer alignment between national preparedness, regional cooperation, NATO deterrence, and EU civilian instruments can the Black

Sea move from being a zone of strategic ambiguity to a space of predictable security, thereby reducing the incentives for hybrid escalation and strengthening the credibility of the Euro-Atlantic security architecture.