CENTER FOR THE STUDY OF DEMOCRACY

COUNTERING WMD HYBRID THREATS AND MALIGN INTERFERENCE IN THE BLACK SEA REGION

Policy Brief No. 141, November 2023

Over the past ten years, the Kremlin has systematically sought to consolidate its influence in the Black Sea region. The Kremlin's geostrategic goals remain identical to those pursued during the Cold War, and achieving supremacy in the Black Sea is a critical prerequisite for attaining these goals. The annexation of Crimea in 2014 was an important signal that Russia's strategy for pursuing geopolitical objectives was changing. The annexation was not preceded by an overt occupation but instead, by the Russian leadership utilising a combination of hybrid measures for internal political interference, including the deployment of a covert military presence that allowed for controlled referenda to take place. In the aftermath of the annexation of Crimea, the Kremlin has persistently supported the insurgent forces in Eastern Ukraine, most notably in the Donetsk and Luhansk regions, thus contributing to a protracted armed conflict and increasing regional destabilisation. Against this backdrop, Russia's invasion of Ukraine in February 2022 constituted a sharp escalation of continuous (and ongoing) belligerent behaviour.

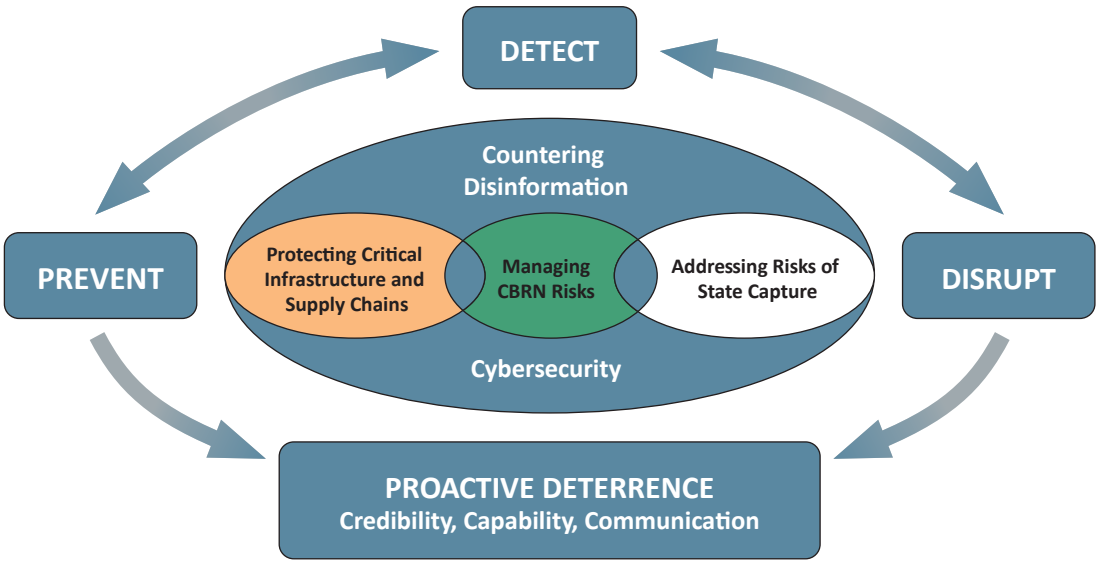
The Black Sea region remains a critical arena in the ongoing war, as the Kremlin strives to convert the region into its own permanent zone of influence. In pursuing this objective, the Kremlin relies on a complex arsenal of tools for interference in and destabilisation of other countries. Moscow deploys these tools in a concerted manner to advance its agenda by fracturing internal unity and integrity within EU and NATO through political manipulation and economic bullying. Bulgaria and Romania are among the most frequent targets of the Kremlin's wide-ranging destabilisation tactics. The two countries have suffered the effects of prolonged Russian malign interference, which has manifested itself in the spread of disinformation and propaganda, cyber-attacks against institutions and critical infrastructure, state capture and political meddling, and encroachment of their exclusive economic zones (EEZ).

KEY POINTS

- The countries in the Black Sea region remain vulnerable to continued efforts by **the Kremlin to consolidate its influence in the region** using tactics that range from hybrid warfare to a full-scale military invasion.
- Strategic corruption, **capture of key economic assets** in foreign countries through regulatory manoeuvres and opaque networks of patronage, exploitation of economic dependencies to gain control over domestic decision-making in target countries, and blatant interference using Soviet-style "active measures" such as information manipulation and targeted assassinations are some of the most common tools of influence that make up the Kremlin Playbook.
- Russia has used **disinformation campaigns** that exploit issues related to weapons of mass destruction (WMD) to target the countries in the Black Sea region as a form of **cognitive warfare** that preys on public anxieties to advance its geopolitical agenda.
- **Black Sea regional security cooperation** and strategic engagement with EU and NATO partners is critical for harmonising the efforts to deter and counter the Kremlin's hybrid warfare strategy and bolster the region's defence capabilities.
- **Media capture** is a key aspect of the Kremlin's disinformation strategy in the Black Sea region. The implementation of national counter-disinformation frameworks that address the risk of media capture is key to ensuring multi-stakeholder coordination, promoting good-quality journalism, and enabling ongoing media monitoring.

This publication was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the author[s] and do not necessarily reflect those of the United States Department of State.

Figure 1. An Integrated Approach to Countering Hybrid Threats



Source: *CSD.*

In the run-up to the unprovoked invasion of Ukraine on 24 February 2022, Russian political and military leadership systematically denied and ridiculed any prospect of a violent confrontation. It might appear as if the war began suddenly but in retrospect, the actions of the Kremlin throughout the escalation of the conflict are characteristic of a carefully planned **strategy that gradually shifted from a hybrid warfare** to a *de facto* **whole-scale invasion**. Political pressure, amassing of troops, military exercises in close proximity to the Russia-Ukraine border, and persistent support for the insurgent groups in Eastern Ukraine were some of the elements of the Kremlin's hybrid warfare strategy. Whilst these strategically motivated methods of coercion and subversion did not amount to an actual armed attack prior to 24 February 2022, they were instrumental in blurring the distinction between war and peace and creating a permanent state of confrontation.

Long before the invasion of Ukraine, the Kremlin has taken steps toward the institutionalisation of hybrid warfare as its primary instrument of foreign policy. **Strategic corruption**, capturing of key economic assets in foreign countries through regulatory manoeuvres and opaque networks of patronage, exploiting economic dependencies to gain control over domestic decision-making in target countries, and blatant interference using Soviet-style "active measures" such as information manipulation and targeted assassinations are some of the most common tools of influence that make up the Kremlin Playbook.[1] Typically **deployed in a concerted manner**, such techniques seek to weaken democratic processes and institutions by eroding their very foundations, including the core values of openness, transparency, pluralism, rule of law, accountability, and civil liberties.

Russia's hybrid warfare strategy preys on societal divisions, the rules of fair competition, and the freedom of expression and media freedom; it juxtaposes security and liberty, radicalises political debates, and capitalises on regulatory loopholes in ways that harm others and undermine their capability for decision-making. The ultimate goal is to influence the patterns of behaviour of the leadership and population in the target country in ways that benefit Russia by manipulating their perceptions of reality. This strategy is not limited to any particular domain; on the contrary, it affects multiple distinct domains such as critical infrastructure, cyber, economy, military/defence, culture, public administration, political, social, and legal affairs, intelligence, and diplomacy. It follows a trajectory of gradual escalation which merges civil and military space across the physical and cyber worlds.

Russia has taken advantage of **emerging technologies to revitalise its hybrid warfare toolbox.** This trend is particularly evident in cyberspace where the Kremlin's army of proxies increasingly uses bots to spread disinformation and propaganda, and carries

[1] Shentov, O., Stefanov, R., and Vladimirov, M. (2020) *The Kremlin Playbook in Europe*. Center for the Study of Democracy.

out cyberattacks against the critical infrastructure and public administration of the countries in the Black Sea region as an expression of power. Russia's offensive cyber activities during the ongoing invasion of Ukraine are frequent and cyber 'spillover' from the war has affected other countries in the region, as well.[2]

Counter measures to address Russia's malign influence in the Black Sea countries must include the development of integrated national strategies for responding to hybrid threats by fostering synergies among relevant government agencies and civil society stakeholders and mobilising resources and expertise for threat monitoring and capacity building (Figure 1). Any such framework must centre on proactive deterrence, in order to ensure capacity for intercepting aggressive behaviour in a timely manner. Proactive deterrence requires credible retaliation options; capabilities such as tools, techniques, and procedures to detect hybrid threats, as well as coordination mechanisms to implement a whole-of-government deterrence policy; and communication that is tailored to the domestic information environment and leverages strategic messaging across government sectors.[3]

Toxic Gambit: The Kremlin's Trail of Poisoning Attacks

The Kremlin's aggressive posture signals a renewed interest in unconventional weapons as a means of power projection. Since the early days of the war against Ukraine, the Kremlin has regularly made explicit references to its nuclear arsenal, and Russia's nuclear forces remain on a higher alert. This follows the Kremlin's use of state-sponsored targeted assassination involving hard-to-detect chemical, biological, or radioactive substances associated with weapons of mass destruction (WMD), which has become a common tactic of Russia's security apparatus. Kremlin-backed poisoning attacks remain below the threshold of an actual armed conflict and are usually carried out covertly rather than overtly. Such attacks constitute a significant deterrence challenge, as they require a drastically altered approach for detection, preparedness, and response in comparison to traditional large-scale WMD attacks. Identifying the perpetrators and bringing them to justice is a lengthy and tedious process which requires that law enforcement services possess appropriate detection and investigation capabilities to respond effectively.

Russia's use of targeted **assassinations through poisoning** undermines the existing concepts of chemical, biological, nuclear, and radiological security in the Black Sea region. Whilst such attacks resemble CBRN terrorism, their motivation and modus operandi differ, not least because states like Russia are far better resourced and prepared to plan, organise, and carry out such violent acts on a frequent basis.

The targets of Kremlin's poisoning attacks vary, but generally these include individuals who oppose or otherwise challenge Russia's unconstrained power and indiscriminate use of force. A recent such case involves Natalia Arno, the founder and president of the Free Russia Foundation who felt sick with multiple organ failure during a trip to Prague in March 2023.[4] Her symptoms corresponded with polyneuropathy – damage of the peripheral nerves. Arno's colleague at the Free Russia Foundation, Vladimir Kara-Murza, survived two poisoning attempts with an unidentified toxin (in 2015 and 2017, respectively) before a Russian court sentenced him to 25 years of imprisonment for treason because of his opposition to the war against Ukraine.[5]

The trail of **poisoning attacks against opponents of the Kremlin** runs long, and includes the targeting of non-Russian nationals.[6] A case in point is Viktor Yushchenko who embarked on a presidential campaign in 2004 in Ukraine. Yushchenko suffered a severe dioxin poisoning whilst running for president against the Kremlin-backed candidate, Viktor Yanukovych. The Bulgarian arms producer Emilian Gebrev, his son and the production director of Gebrev's company were poisoned with a chemical nerve agent, similar to Novichok, in 2015. Years later, the Bulgarian Prosecution Office announced

[2] See, for example, Fendorf, K. and Miller, J. (2022) Tracking cyber operations and actors in the Russia-Ukraine war, *Blog Post,* Council on Foreign Relations, 24 March; Rosca, M. and Fota, A. (2022) "Romania hit with cyberattacks at start of Ukraine war, official says", *Politico,* 15 March.

[3] See Monaghan, S. et al. (2019), *Countering Hybrid Warfare,* Multinational Capability Development Campaign Project.

[4] KennanX Episode 29: Surviving a political poisoning with Natalia Arno, 14 September 2023, Wilson Center.

[5] Eckel, M. (2021) "New FBI documents shed light on probe into Russian activist's near-fatal illnesses", *Radio Free Europe,* 7 September; UN Office of the High Commissioner for Human Rights. (2023) "Russia: Kara-Murza's continued detention threatens his life and violates his human rights, says UN expert", *Press release,* 28 July.

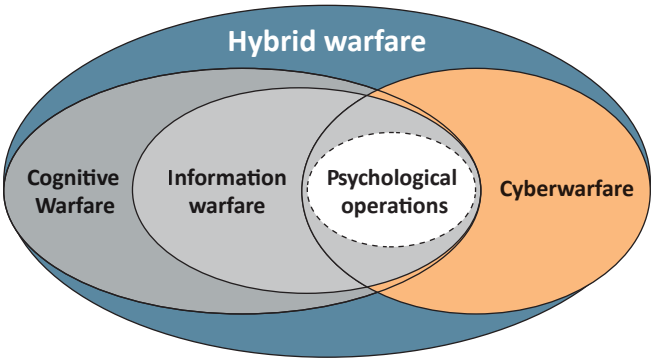
[6] Foltynova, K. (2020) "A timeline of Russian poisoning cases", *Radio Free Europe,* 8 October.

indictments for three GRU officers, releasing key evidence including the group's hotel record and security camera footage.[7] In addition, since 2011, there have been several cases of explosions under suspicious circumstances in warehouses of Gebrev's company in both Bulgaria and Czechia.[8] Gebrev's investigation led to revelations that have helped link his case to the Novichok attack against the Russian former double-agent, Sergei Skripal, in Salisbury, England.

Russia's Cognitive Warfare in the Black Sea Region

Cognitive warfare plays an important role in the Kremlin's hybrid warfare strategy (Figure 2). It encompasses a broad range of activities that seek to produce self-replicating models of social cognition and behaviours which promote and reinforce Russia's political, economic, and socio-cultural agenda. The Kremlin's cognitive warfare is **complex and multifaceted,** combining traditional techniques and instruments of influence – e.g. psychological and information operations, social engineering – with cyber and other advanced technological capabilities. It is designed and deployed as an **indiscriminate tool** that can target entire populations by leveraging emerging information and communication technologies. The use of cognitive warfare tactics enables the Kremlin and its proxies to influence how beliefs about political, economic, and socio-cultural issues are formed and maintained, and the end-goal of this approach is the destabilisation of democratic institutions and processes. Because of its broad scope and far-reaching objectives, Russia's cognitive warfare should be treated as a distinct operational domain.

Figure 2. Information Domains in Hybrid Warfare



Source: *CSD.*

Disinformation campaigns are an important instrument of Russia's foreign policy. These campaigns are multifaceted and versatile exploiting a wide range of issues and conducted through multiple channels, involving the active participation of proxies and agents of influence. Russia's disinformation activities are multi-layered, effectively blurring the distinction between state and non-state actors and hindering the process of attributing specific malign actions to Russian political leadership.

The Kremlin's disinformation strategy in the Black Sea region both relies on and aims at **projecting economic influence** to solidify control over key assets. **Media capture** is but one example of how Kremlin-sponsored networks leverage regulatory, institutional, and procedural arrangements in target countries to infiltrate the media space and gradually seize and ensure full control over political decision-making and public agendas.[9] Media capture concerns both the **material aspects** of the media sector, i.e. the business arrangements, ownership structures, and financial flows of media companies, and the **ideational aspects**, namely the content and editorial policies of outlets, as well as the overriding perceptions among managers, editors, and journalists. What unites these two strands in the Kremlin's media capture strategy is the overarching objective to discredit democratic systems of governance and disrupt the functioning of their associated processes and institutions.

Against this backdrop, **Russia's disinformation campaigns that exploit CBRN-related topics** are blatantly malign, as they prey on public fears and anxieties and can result in individuals adopting risk-prone behaviours. This trend manifested itself vividly during the COVID-19 pandemic, when Russian disinformation efforts specifically targeted American and European vaccination campaigns in an attempt to encourage the uptake of Russian-made vaccines.[10] Through the active dissemination of fake data and conspiracy theories, Kremlin-sponsored and pro-

[7] "Post-Mortem of a Triple Poisoning: New Details Emerge in GRU's Failed Murder Attempts in Bulgaria". *Bellingcat*, 4 September 2020.

[8] "How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine". *Bellingcat*, 26 April 2021.

[9] Georgiev, G., Petrova, V., and Tsabala, K. (2023) *Breaking the code: tackling the interlocking nexus of Russian and Chinese disinformation and illicit financial flows in Southeast Europe*, Center for the Study of Democracy.

[10] Barnes, J. (2021) "Russian disinformation targets vaccines and the Biden Administration", *New York Times,* 5 August.

Kremlin groups have sought to sow doubts about the safety and reliability of "Western" vaccines, contributing in some instances to low vaccination rates.[11] Another prominent set of disinformation messages that populated the media space in Bulgaria and Romania concerns the proliferation of conflicting explanations of the origin of the COVID-19 virus: namely, that it originated as an American biological weapon; that 5G technology caused it; or that the global economic elite engineered it to conceal a global economic crisis that had already been under way.[12] Russian disinformation messaging has also strived to ascertain that authoritarian regimes are allegedly better able to cope with the pandemic crisis than liberal democracies because centralized systems can mobilize a quick response and harness industrial capacity for the production of medical equipment.

On other occasions, the Kremlin has mobilised its disinformation and propaganda machinery to **divert attention from and cover up state-sponsored belligerent activities** such as CBRN-enabled targeted assassinations. Pro-Kremlin disinformation narratives regarding the poisoning of Emilian Gebrev that abounded in the Bulgarian media space have sought to cast doubt on the facts of his poisoning and question the veracity of Western accounts of the incidents. Such narratives have focused on questioning the chemical agent that was used in the assassination attempt and painting the incident as part of an anti-Russian smear campaign by Western forces.[13]

From the outset of the war against Ukraine, Russia has relied on nuclear blackmail and the spread of disinformation and false flag alerts that Ukraine has sought to acquire nuclear weapons or use a "dirty bomb".[14] The ongoing occupation of the Zaporizhzhia Nuclear Power Plant (NPP), the largest in Europe, by the Russian armed forces remains a cause of public concern, as it compromises nuclear safety and security in the Black Sea region.

Yet the Kremlin's **disinformation campaigns extend well beyond the media space** to target existing international decision-making mechanisms, including the United Nations Security Council. Shortly after the invasion of Ukraine in February 2022, the Kremlin claimed that Ukraine and the United States violated the **Biological and Toxin Weapons Convention** (BTWC). Ukrainian biomedical research laboratories, which play an essential role in the local system for public health and disease prevention, were the prime target of this campaign. This strategy itself is not new; the Kremlin has long used the same approach to discredit **Georgia's national reference laboratory**, the Lugar Center. As part of its disinformation campaign on the work of biological laboratories in Ukraine, Russia invited a Bulgarian journalist, Dilyana Gaytandzhieva, as a briefer to a high-level meeting within the framework of the UN Security Council; Gaytandzhieva's work has regularly aligned with parallel Russian information operations.[15] Gaytandzhieva describes herself as a Middle East Correspondent who received leaked diplomatic documents about arms shipments to terrorist organisations while reporting on the Syrian civil war. Her reporting at the time shows that she enjoyed unlimited access to Russian-controlled territories in Syria. Gaytandzhieva has actively advanced pro-Kremlin narratives accusing Georgia and Ukraine of developing biological weapons with American funding. Her articles have appeared on *SouthFront*, an outlet that was sanctioned by the U.S. Treasury Department in 2021 and 2022 for propagating Russian intelligence services-directed content.

Pro-Kremlin disinformation messaging in the online media space in Bulgaria and Romania has sought to amplify the allegations of bioweapon development in Ukraine coming from high-level political figures in Russia and Kremlin-controlled media. Some of the most common disinformation narratives include that the United States runs labs in the post-Soviet space to develop weapons of mass destruction; that the United States is collecting biological materials from Russian citizens to create a new generation of biological weapons; and US-funded labs in Ukraine were engaged in the production of the COVID-19 virus.[16] The reprinting of content produced

[11] Gordon, M. and Volz, D. (2021) "Russian disinformation campaign aims to undermine confidence in Pfizer, other Covid-19 vaccines, U.S. officials say", *Washington Post,* 7 March.

[12] Filipova, R. et al (2020), The shrinking space for media f*reedom in Southeast Europe in the midst of the COVID-19 pandemic and state of emergency,* Center for the Study of Democracy.

[13] For further discussion on this point, see *Russia's hybrid threats toolbox: pro-Kremlin media narratives surrounding a suspected Russian chemical weapons attack on Bulgarian soil,* FENCE Flash report, 23 February 2023.

[14] See Sinovets, T. et al (2023) "Russia's disinformation goes nuclear", *Forum for Ukrainian Studies,* 23 March.

[15] Mejia, L. et al (2022) "Telling on themselves: indicators from Kremlin disinformation in Ukraine", Microsoft Threat Analysis Center, 10 March.

[16] See Malinov, S. (2022) *Disinformation narratives in the Bulgarian online media: the US accused of setting up bio labs in the post-Soviet space,* FENCE Flash report, 14 March; Raducu, R. and Hercigonja, S. (2023) *Disinformation in the context of the Russian invasion of Ukraine: narratives used by the Russian propaganda in the Balkans.* West University of Timișoara; Gombos, G. (2023) "(Pro-)Russian propaganda sees connections between biological weapons and the Nova Kakhovka dam", *Verdica,* 11 October.

by Russian sources, including by Russian media outlets that are under sanctions, is a regularly utilised practice by which disinformation narratives penetrate the Bulgarian online media space. The social media footprint of the Russian embassies in countries in the Black Sea region like Bulgaria and Romania is another important enabler for projecting information influence.[17] Moreover, the integration of formal (e.g. high-level political statements) and informal platforms (e.g. pages and groups on social media) provides for the rapid and *en masse* dissemination of Kremlin-favoured disinformation narratives and fake news.

What's Next?

Crafting an effective strategy to counter Russia's hybrid warfare tactics in the Black Sea region requires action on multiple fronts and across different sectors. The Kremlin's renewed interest in CBRN-enabled attacks is unlikely to subside; however, securing access to cutting-edge knowledge, technologies, and equipment is likely to run into hurdles as a result of sanctions and the already crippled Russian economy. In the context of increasing international isolation, Russia may grow more determined to activate its entire arsenal of instruments of influence to probe into new markets and take control of key assets in foreign countries. The Black Sea region is particularly vulnerable in this regard, not least because Russia's ongoing aggression in Ukraine has further emboldened Moscow to challenge the NATO Eastern Flank. Enhancing societal resilience against pro-Kremlin disinformation and its modus operandi in the countries in the Black Sea region is an essential prerequisite for confronting the Kremlin's cognitive warfare activities.

- **Strengthening Black Sea regional security cooperation and cooperation within the EU and NATO**. Black Sea regional security cooperation and strategic engagement with EU and NATO partners is critical for harmonising efforts to deter and counter the Kremlin's hybrid warfare strategy and bolster the region's defence capabilities. Joint training initiatives and exercises, implementation of intelligence, surveillance, and reconnaissance systems for threat monitoring and early warning, and defence modernisation are essential for increasing NATO interoperability and reinforcing its posture in the Black Sea region.

- **Fostering economic and energy security**. Initiatives that promote investment screening,[18] transparency in public procurement,[19] and diversification of sources, routes, and types of energy supply[20] are key to mitigating the risk of political coercion through economic dependencies in the Black Sea region. Effective implementation and compliance with the sanction regimes adopted in response to Russia's use of Novichok and its war of aggression against Ukraine play an important role in hindering the Kremlin's military expansion and limiting Russia's potential for carrying out hybrid warfare activities.[21]

- **Developing an integrated national strategy for responding to hybrid threats**. Implementing an integrated and comprehensive national strategic framework for tackling hybrid threats enables countries in the Black Sea region to develop synergies among relevant government agencies and civil society stakeholders and mobilise resources and expertise for threat monitoring and capacity building.

- **Keeping national procedures and protocols for detection, preparedness, and response to CBRN security threats up-to-date**. To address the risk of CBRN-enabled targeted assassinations, it is important that countries in the Black Sea region regularly review and update, as appropriate, their national policy, regulatory, strategic, and operational documents for prevention, investigation, and response to deliberate CBRN acts.[22] Intelligence and data sharing and cooperation among competent authorities including law enforcement agencies is essential for countering any form of malign interference by the Kremlin.

[17] See O'Kelley, C. (2023) *Russian embassy Facebook activity in Southeastern Europe,* FENCE Flash report, 28 February.

[18] See, for example, Boycheva, I. and Terziev, P. (2022) *Investment Screening in Bulgaria: Policy Options, Institutional and Legal Framework,* Center for the Study Democracy; *Investment Screening in Bulgaria*, Policy Brief No.123 (2023), Center for the Study of Democracy.

[19] See *The State of Capture: The Risks to Distributive Politics in Southeast Europe,* Policy Brief No. 139 (2023), Center for the Study of Democracy.

[20] See *Moving Forward Together: Energy and Climate Security for Ukraine and Europe,* Policy Brief No. 136 (2023), Center for the Study of Democracy.

[21] See, for example, *Sanctions Evasion and Derogation on Russian Oil,* Policy Brief No. 140 (2023), Center for the Study of Democracy.

[22] *Countering Hybrid Threats in Bulgaria,* Policy Brief No. 118 (2022), Center for the Study of Democracy.

- **Strengthening institutional capacity at the national level to combat media capture and disinformation**. Media capture is a key aspect of the Kremlin's disinformation strategy in the Black Sea region. The recently adopted Digital Services Act (DSA) and Media Freedom Act are central elements of the EU approach to respond to the threat of foreign information manipulation and interference (FIMI) and enhance democratic resilience and both contain provisions for safeguarding the media space against abuse, including the spread of disinformation and propaganda. The development and implementation of appropriate national regulatory and institutional frameworks that tackle the risk of media capture is key to ensuring multi-stakeholder coordination for disrupting disinformation activities, promoting good-quality journalism, and enabling ongoing media monitoring.[23] Establishing well-staffed and resourced strategic communications units within EU and NATO member governments is essential for the timely assessment, detection, and countering disinformation threats.

[23] See *Building Institutional Capacity Framework for Resilience to Disinformation in Bulgaria,* Policy Brief No 131 (2023), Center for the Study of Democracy.