CENTER FOR THE STUDY OF DEMOCRACY

COUNTERING HYBRID THREATS IN BULGARIA

Policy Brief No.118, November 2022

Russia has long prepared its war in Ukraine by deploying the **full array of hybrid warfare tools** at its disposal in Europe: election meddling and strategic corruption aimed at political parties and media, cyber-attacks on critical infrastructure and disinformation, economic coercion, and targeted assassinations using difficult-to-detect toxic agents, to name a few. Europe has been slow to react, with EU member states failing to anticipate the war in Ukraine even after the Kremlin started preparations for its final act by deliberately reducing gas storage levels in Germany in the autumn of 2021. Some EU and NATO member states and many political party leaders across the continent remain in denial, even as the war approaches a full year of destruction. NATO and European institutions have begun to prepare policy and operational responses to these emerging hybrid threats, but implementation remains slow and uneven.

Over the past two decades, Russian security services have been implicated in a series of high-profile cases in which **radioactive and chemical warfare agents were used** to poison individuals perceived as adversaries and political opponents (Figure 1). The most well-known of these cases is the 2006 assassination of Alexander Litvinenko, a Russian defector and dissident, for which the Kremlin's involvement was confirmed in court.[1] The investigations of the Novichok poisonings of the former Russian spy, Sergei Skripal, and opposition leader Alexei Navalny indicate that these incidents have followed a similar pattern to that of Litvinenko. While targeted assassinations are not a novel tactic in the Kremlin's toolbox for power projection *per se*, the use of toxic substances traditionally associated with chemical and nuclear weapon programs signals Moscow's determination to both maintain and deploy its offensive WMD capability, when deemed necessary.

[1] See European Court of Human Rights, *Carter v. Russia*, no. 20914/07, September 21, 2021.

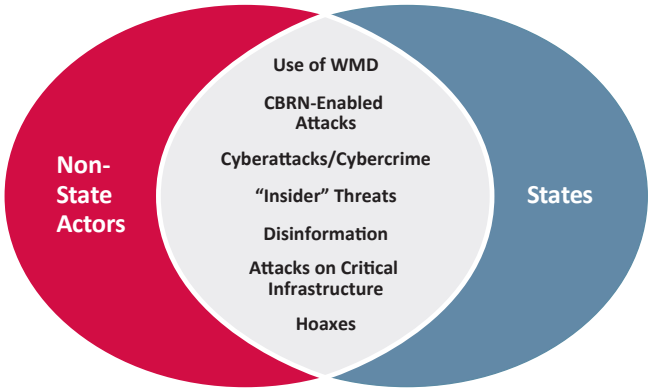
KEY POINTS

- Long before Russia's actual incursions in 2014 and 2022, the Kremlin began to prepare for its **war of aggression** against Ukraine by perfecting a **playbook of hybrid warfare tools**. Russian security services have been implicated in criminal activities against **defense industrial sites** and the usage of **radioactive** and **toxic chemical agents** to target adversaries of the Kremlin's interests throughout Europe. This has come on top of Russian **threats** to use **nuclear weapons** and the spread of **disinformation on biological research activities** in Ukraine.
- Southeast Europe **remains among the most vulnerable regions** to such hybrid threats in Europe. Since February 2022, the Kremlin has intensified its **disinformation campaign**, focusing in particular on technically specific and malign narratives around nuclear and biological weapons.
- Bulgaria's **gaps in operational and technical preparedness and capacity** to counter weapons of mass destruction-related hybrid threats has been compounded by state and media capture and political instability.
- The Bulgarian government must upgrade its institutional capacity and coordination. If Bulgaria can achieve this benchmark, it will be able to detect, prevent, and respond to the full array of hybrid threats including those involving the use of weapons of mass destruction.
- As a matter of urgency, the Bulgarian institutions must focus on **addressing ongoing disinformation and cyberattacks** on the country and its critical infrastructure.

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.

Europe's southeastern flank, and Bulgaria in particular, have remained vulnerable and unprepared to respond to the rising Russian threat in the region. **State and media capture have enhanced the Kremlin's reach and impact** in the region, while hindering or altogether blocking response capabilities and weakening resilience. Protracted political instability and strategic ambiguity have further dampened willingness and readiness to act. This has been particularly true in the area of weapons of mass destruction-related (WMD) hybrid threats, which require complex inter-institutional cooperation on the national and international level and substantial technical capacities and resources.[2]

Figure 1. Types of WMD-related Hybrid Threats



Source: *CSD et al., Countering the Misuse of CBRN Materials and Knowledge, 2022.*

In the past decade alone, Bulgaria has been the target of hybrid attacks of various kinds including WMD-related. The attempted poisoning of the owner of Bulgaria's largest producer and trader of ammunition and weapons capable of strengthening Ukraine's defenses, happened precisely when the same Russian GRU agents who carried out the infamous Skripal poisoning in the UK were present in Bulgaria. There have been numerous explosions and other suspicious incidents in different facilities owned by the country's military industrial complex, and Bulgarian critical infrastructure and public and private institutions have suffered a tsunami of cyberattacks, which have intensified after Russia's invasion of Ukraine in February 2022. The Kremlin has also increased WMD-related disinformation about US biological experiments with Bulgarian army personnel in the Military Medical Academy.[3] In October 2022, the pro-Kremlin hacker group known as Killnet conducted a series of distributed denial of service (DDoS) attacks against government ministries and critical infrastructure; the servers and websites of the Center for the Study of Democracy were also targeted as part of these attacks.[4]

Hybrid Threats in the Kremlin Playbook

Hybrid warfare comprises the coordinated deployment of coercive or subversive measures with the goal of destabilizing an adversary and advancing one's own agenda.[5] Such campaigns can utilize a combination of tactics and tools – e.g. diplomatic, military, technological, and economic – whilst remaining below the threshold of an actual armed conflict, which in turn makes them difficult to detect or attribute. Just like terrorist attacks, hybrid warfare operations can have far-reaching pernicious effects upon the victim state, resulting in loss of life, injuries, damage, disruption of essential services, or widespread panic.

State-sponsored hybrid campaigns can also affect societies in more intangible ways – for example, by gradually **weakening key institutions** in the target country (through systematic corruption or by exploiting regulatory vulnerabilities), **taking over entire sectors of the economy**, undermining established governance processes and arrangements, and polarizing communities. A perfect example of this process is the cycle of state capture that Russia has used to influence strategic foreign policy decisions in Europe (Figure 2).[6]

The two primary channels of the Kremlin's state capture power consist of its state-sponsored networks of influence and corruption and its control over Russia's economic and financial flows. Hard, sharp, and soft power are all part of the Kremlin's toolbox of instruments for influence, leaving target countries exposed to a complex arsenal of wide-ranging tactics intended

[2] Weapons of mass destruction (WMD) include chemical, biological and nuclear weapons. WMD hybrid threats also include the use of chemical, biological, radioactive, and nuclear (CBRN) materials or agents for purposes that are prohibited under international law.

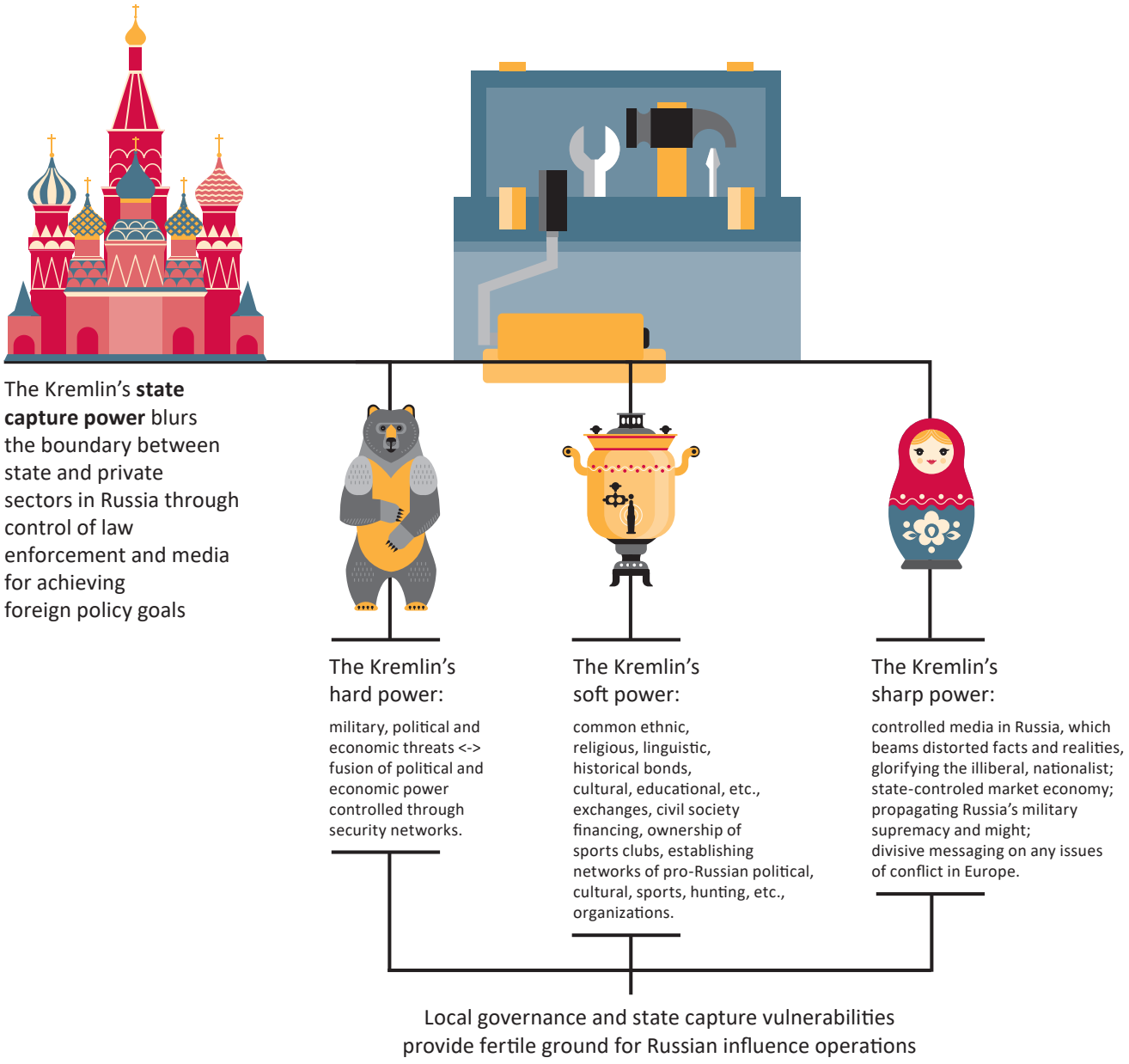
[3] Vasileva, K., „Не, Пентагонът не прави биоексперименти с български войници" [No, the Pentagon does not do bioexperiments with Bulgarian soldiers], *Factcheck.bg*, March 10, 2022.

[4] *We are Killnet*, 15 October 2022.

[5] European Commission, *Increasing resilience and bolstering capabilities to address hybrid threats*, Brussels, 13.6.2018, JOIN(2018) 16 final.

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

Figure 2. Kremlin Playbook – Toolbox Instruments



Source: *CSD, Kremlin Playbook in Europe, 2020.*

to guarantee long-term control over key local assets and policymaking initiatives.[7]

Russia's media capture strategy combines media ownership, control over advertising budgets, and coordination and support for journalistic proxies that manufacture fake news to promote disinformation narratives.[8] As an evolution of Cold War-era 'active measures', media capture has allowed the Kremlin to amplify its influence in Europe considerably through the deployment of coordinated disinformation and propaganda campaigns. These methods exploit political indecisiveness and public opinion ambiguities regarding strategically significant issues in such areas as national security, energy, and foreign policy. They thus cover all four elements of media capture in Bulgaria:

- **Ownership capture**: Many Russia-sympathetic media outlets have been owned by individuals and businesses with strong commercial and other ties to Russia. Before the war in Ukraine, Russian state-owned propaganda channels were readily and widely available to Bulgarian viewers. In addition,

[7] Stefanov, R. et al., *The Kremlin Playbook in Southeast Europe*, Sofia: Center for the Study of Democracy, 2020.

[8] Shentov, Stefanov, and Vladimirov (eds.), *The Kremlin Playbook in Europe*, Sofia: CSD, 2020.

Russia-controlled entities owned numerous media outlets nationally, in particular along the Black Sea coast.

- **Advertising capture**: Many Bulgarian companies, in particular in the energy sector, have such well-known ties to Russia that media outlets would carefully weigh the risks reporting anything critical about their benefactors. Some of the largest and most active corporate advertisers in Bulgaria have been Russia-controlled entities, such as Lukoil, VTB, etc.

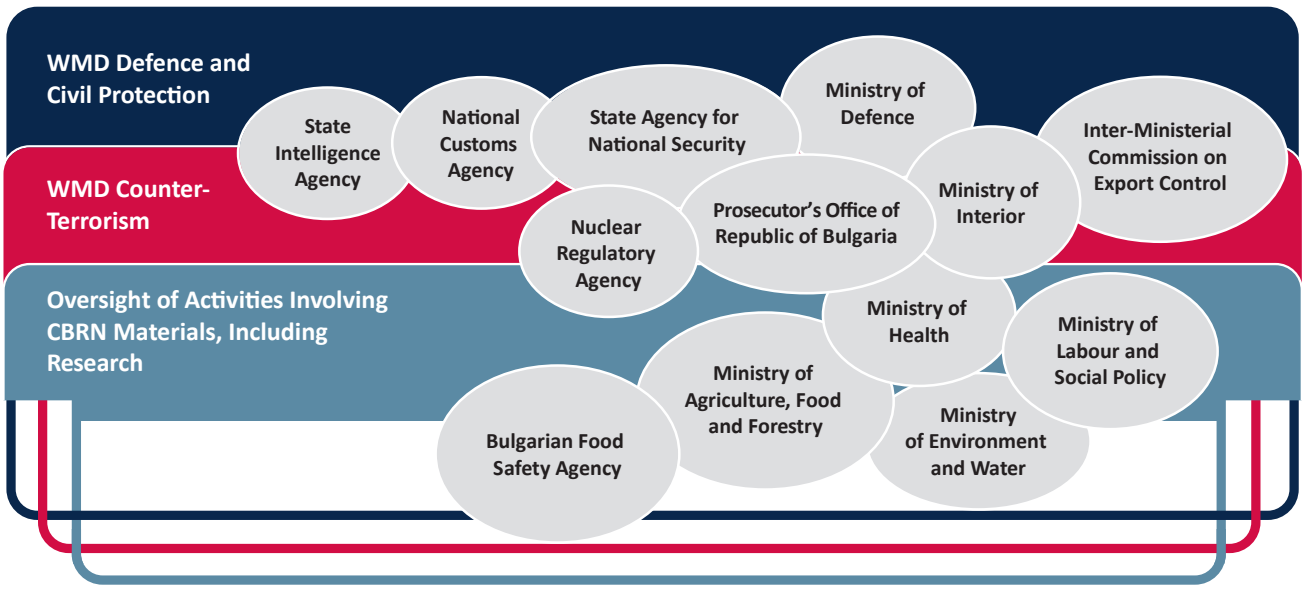
- **Government capture:** Likely the most important factor for the penetration and the persistence of pro-Russian disinformation in the Bulgarian media space is the ambiguity or sometimes even the lack of response towards Russia's aggressive behavior from the highest political level in the country. Current and former prime ministers, cabinet ministers, and presidents have repeatedly tried to "balance" their public attitude towards Russia and its perceived interests in Europe against the interests of NATO and the EU. Parties represented in parliament have directly parroted pro-Russian disinformation narratives. This strategic ambiguity has trickled down along all media channels in the country, including first and foremost the three major national TV channels.

- **Cognitive capture:** Bulgarians have long ranked among the most Russia-sympathetic peoples globally. This positive attitude towards Moscow is reinforced by strong historical, cultural, religious, and linguistic ties, and has been practically embedded in all political, social, economic, defense, and security during the Cold War. Cognitive capture directly affects the country's political landscape; Bulgarian political parties have been locked in competition to win the votes of the over 25% (and counting) of the population which have remained staunchly pro-Russian, even after the start of the war in Ukraine.

The Kremlin's Hybrid Threats targeting Bulgaria

Responding to WMD-related hybrid threats and disinformation in Bulgaria must be **integrated into a much wider policy reaction** to the Kremlin Playbook (Figure 3). Proper understanding of the depth and scope of Kremlin's current hybrid threat operations requires knowledge about the wider Kremlin Playbook of Russian influence in Europe; this influence is based and feeds on **state capture networks** and practices that predate Bulgaria's democratic transition. It also relies on **media capture** that is much deeper and more complex than the level and breadth of current disinformation activities. Ultimately, the Kremlin Playbook is borne out of long-lasting economic and technological dependencies with their roots in the energy and military industrial complex.

Figure 3. Bulgaria's Institutional Framework for Countering WMD-related Threats



Source: *CSD.*

Despite being a NATO member for nearly 20 years now, **Bulgaria remains among the Kremlin's preferred targets** for hybrid warfare campaigns. The 2015 poisoning of Emilian Gebrev, the owner of one of Bulgaria's largest defense industrial companies, is a prime example. Gebrev's case provides a useful overview of the full array of Kremlin tools deployed in Bulgaria, as well as the capacity of national institutions to respond effectively. His companies' storage facilities have also been targeted on multiple occasions since at least 2010.

Bulgaria is the second-largest exporter of ammunition in Eastern Europe after Russia, and has been one of the most significant exporters of Soviet-standard ammunition, small arms, and light weapons destined for Ukraine.[9] In 2020, the Prosecutor's Office in Bulgaria accused three operatives of the GRU, an arm of the Russian intelligence service, of attempted murder.[10] One of the accused persons is also implicated in the 2018 Skripal poisoning. **The charges were brought forward only after UK authorities** officially and publicly alerted their Bulgarian counterparts to the obvious similarities in the two incidents. Previously, Bulgarian authorities had been hesitant to launch an investigation into the poisoning, even though the incident had been formally detected in the Military Medical Academy, an official WMD-response facility, and confirmed by an independent analysis from an internationally accredited laboratory.

Interestingly, the case also holds a number of circumstantial evidence indicators, revealing how Bulgaria's state and media capture affects its **capacity to respond to such complex threats**. Since 2014, Gebrev had been locked in an existential battle over the control of one of his military factories with Mr. Delyan Peevski, a former Bulgarian media mogul and member of parliament, sanctioned in 2021 by the U.S. administration under the Global Magnitsky Act. The same factory became infamous thanks to another plot involving Russia. In 2019, Bulgarian prosecution services detained Nikolay Malinov, the leader of the Russophile movement in Bulgaria, on espionage charges. A critical piece of evidence from the case, shared publicly by the Bulgarian prosecution, showed that Malinov had written to the Russian ultra-orthodox Putin supporter Konstatin Malofeev, proposing a plan of action for acquiring critical economic assets in Bulgaria to return the country to the Russian sphere of influence.[11] One of the assets proposed for acquisition was Gebrev's factory.[12] While the espionage investigation was still ongoing, a judge allowed Malinov to travel to Moscow to receive a medal from Putin without properly notifying the Bulgarian prosecution. Subsequently, the judge was sanctioned by the U.S. Department of State.

In addition to this development, the Gebrev case has been continuously inundated by disinformation. Gebrev's poisoning has featured extensively in the Bulgarian pro-Kremlin online media space, where it was claimed that the poisoning was:

- An accident as a result of consuming contaminated food.
- Connected to his activities as a clandestine arms trafficker for the CIA.
- Carried out by local oligarchic competitors who hired Russian intelligence operatives to conduct the poisoning.
- Fabricated to worsen relations between Bulgaria and Russia.
- Fabricated by the Western media to discredit the Russian intelligence service by referring to a unit (i.e. GRU Unit 29155) that does not exist.

What's Next

Bulgaria must carry out a full assessment of its capacity to counter hybrid threats, and prepare an actionable plan for long-term capacity sustainability (Figure 4). Building resilience to the hybrid threats posed by Russia requires effective action on multiple levels. International cooperation within bodies such as the EU and NATO is essential for the development of a

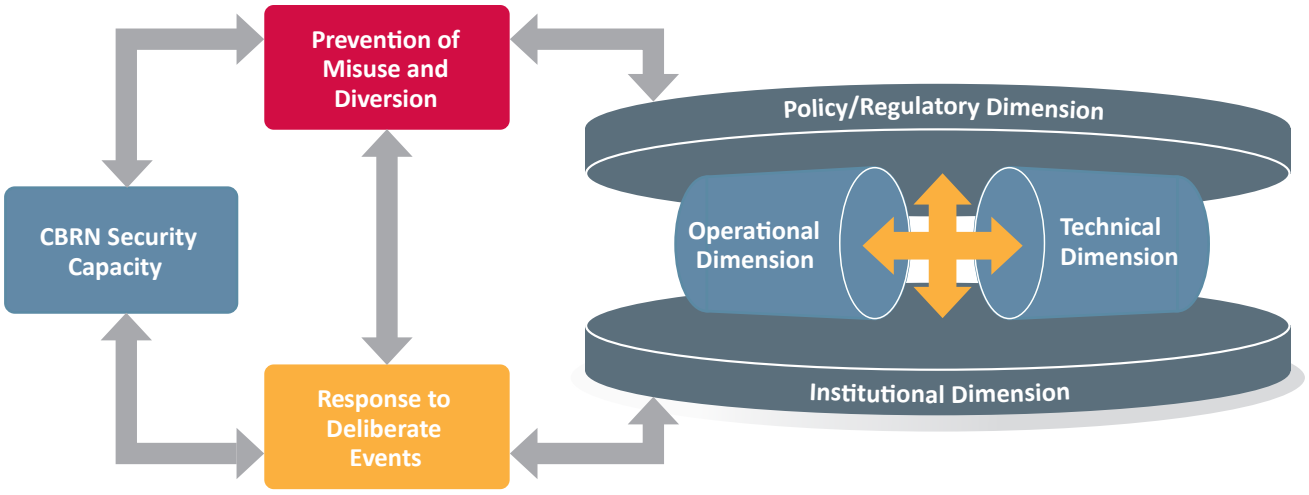
[9] Gospodinova, V., and Yurdanov, A, „Оръжията на раздора" [Weapons of Discord], *Capital*, April 26, 2022; Bloomberg TV Bulgaria, „Безлов: Има голям износ на боеприпаси от България за Украйна през трети страни" [Bezlov: There is significant exportation of ammunitions from Bulgaria to Ukraine through third countries], May 5, 2022.

[10] This press release concerns an ongoing investigation. See Prosecutor's Office of the Republic of Bulgaria, „СГП предоставя информация по досъдебно производство за отравянето на Ем. Гебрев, Хр. Гебрев и В. Тахчиев" [Press release of the Sofia City Prosecutor's Office regarding the pre-trial proceedings on the poisoning of E. Gebrev, H. Gebrev, and V. Takhchiev], September 15, 2020.

[11] Trichkova, V., „Прокуратурата разпространи доказателства по шпионския скандал (ОБЗОР)" [The Prosecutor's office releases evidence in spy scandal (VIDEO)], *Nova TV*, September 12, 2019.

[12] Webcafe, „Прокуратурата публикува уликите срещу Николай Малинов" [The Prosecutor's office published the evidence against Nikolay Malinov], September 12, 2019.

Figure 4. Capacity Assessment Methodology for Countering WMD Use



Source: *CSD et al., Countering the Misuse of CBRN Materials and Knowledge, 2022.*

unified and robust approach to countering foreign malign influence operations, capable of deterring the use of disinformation as a weapon. Good governance and **resilient institutional and digital security infrastructure** is a first line of defense and an essential precondition for preventing state and media capture and countering hybrid threats. **Preventive measures,** besides typical counterintelligence and counterterrorism measures, include initiatives and campaigns to enhance media literacy and public sensitivity to social manipulation (e.g. fact-checking), efforts to strengthen strategic communication, and standard-setting initiatives that advance quality journalism and responsible media coverage. Enforcing regulatory compliance to promote the **transparency of media ownership and funding** is a key step toward improving the media landscape within countries and reducing the risk of media capture.

An effective regulatory and institutional framework for preventing and countering WMD hybrid threats at the national level should, *inter alia*:

- Be based on a whole-of-government, cross-thematic approach to dealing with influence operations that fosters coordination among government agencies and tackles the technical (e.g. cybersecurity) as well as political-economic aspects of foreign disinformation activities.

- Provide for the periodic review of the policy and legal instruments aimed at combating the misuse of WMD/CBRN materials, as well as any related information, to ensure that the established mechanisms and provisions are up-to-date.

- Ensure that security-sector institutions, including those responsible for intelligence-gathering, law enforcement, and criminal justice, are well-resourced and equipped to identify, detect, investigate, and prosecute incidents involving the use of WMD/CBRN materials.

- Promote inter-agency cooperation and inter-operability during the response and investigation of suspected use of WMD/CBRN materials.

- Guarantee the availability of technical infrastructure, equipment, and expertise necessary for identifying and analyzing suspected use of WMD/CBRN materials.

- Ensure that strategic communications units on the ministerial and local governance level are well-equipped to raise awareness and clarify policy initiatives aimed at combating disinformation in a timely and consistent manner.

- Leverage specific social media capabilities in the national language and promote cooperation with major social media platforms and national IT associations to foster shared understanding of external threats.

- Adopt technology solutions via public-private partnerships with the IT sector to detect and investigate recurrent disinformation and the actors that produce and amplify it.

- Establish mechanisms for cooperation and exchange of information with civil society, including academia, to facilitate the analysis of disinforma-

tion threats and the identification of options to effectively counter them.

Civil society, including the private sector, plays a vital role in ensuring wide access to trustworthy and verifiable information, quality reporting, and media monitoring.[13] Key initiatives that civil society stakeholders can undertake include:

- Developing fact-checking tools and platforms to facilitate the identification of disinformation narratives.
- Adopting and promoting voluntary (self-regulatory) mechanisms for reporting disinformation and strengthening ethical and responsible journalism.
- Developing, implementing, and popularizing technological solutions and data-driven methods for analysis and media monitoring to identify recurrent disinformation narratives.
- Enhancing public engagement to raise awareness of disinformation threats, and to demonstrate how these threats can be addressed and countered.
- Establishing a platform for the development of sustainable business models for independent media.
- Developing tools and resources for teaching information literacy, geared to various target audiences.

[13] Center for the Study of Democracy, *Policy Agenda for Countering Media Capture in Europe*, Policy Brief No. 116, 2022.