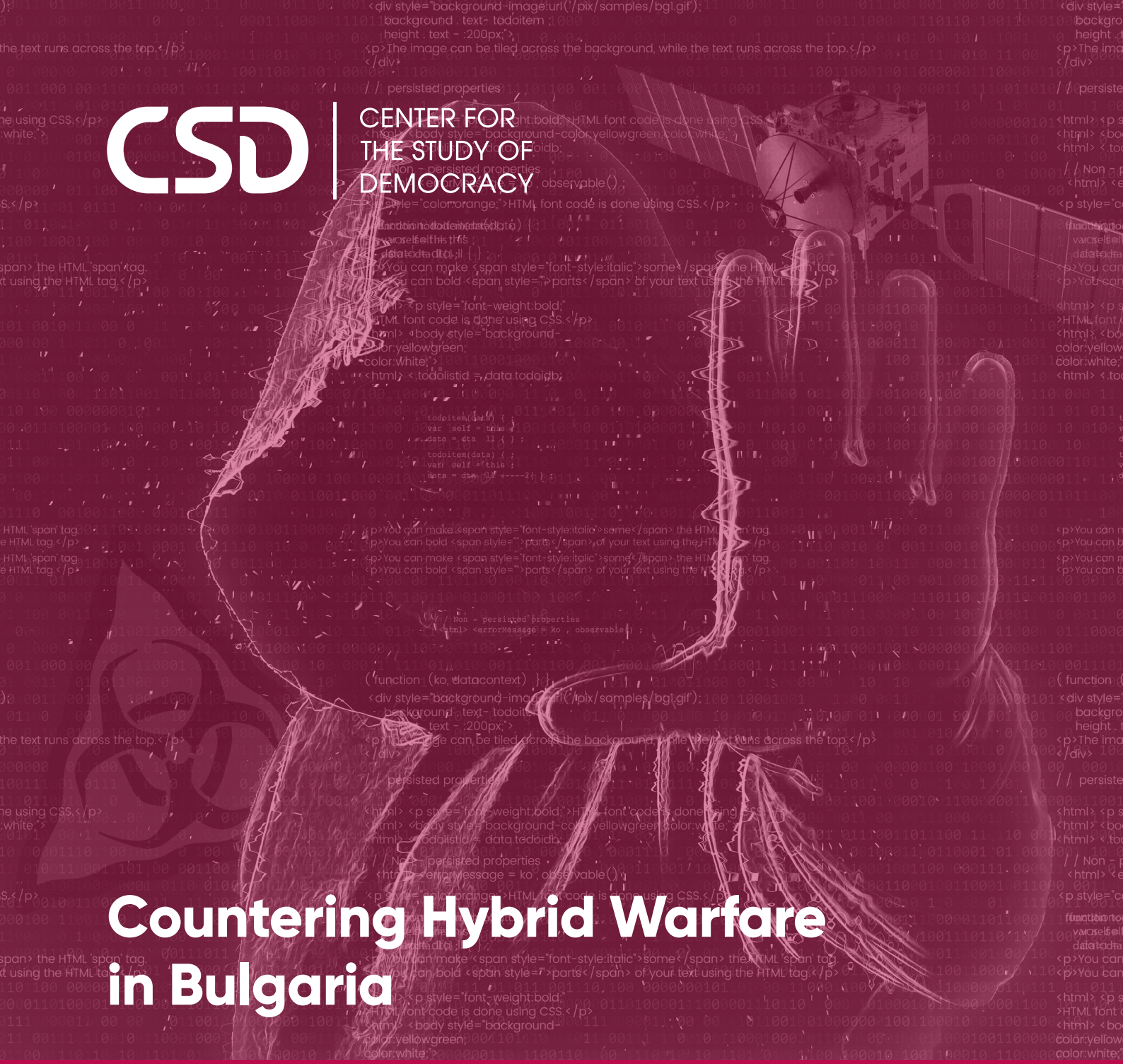
CSD | CENTER FOR THE STUDY OF DEMOCRACY



# Countering Hybrid Warfare in Bulgaria

A Strategic Assessment
of National Capabilities and Infrastructure

# Countering Hybrid Warfare in Bulgaria

## A Strategic Assessment of National Capabilities and Infrastructure

CSD
CENTER FOR THE STUDY OF DEMOCRACY

Bulgaria has been among the preferred targets of Russia's influence operations, which employ hybrid warfare tactics, combining hard, soft, and sharp power. This report outlines a model of an integrated national approach for preventing, detecting, and disrupting hybrid threats. The model centres on proactive deterrence, in order to ensure capacity for intercepting aggressive behaviour in a timely manner. The report maps key competent authorities and initiatives undertaken by civil society stakeholders in Bulgaria in four cross-cutting areas of action: countering disinformation; cybersecurity; resilience of critical infrastructure and supply chains; and emergency and crisis management and defence.

The development of this report is part of an initiative on *Countering WMD Hybrid Threats in the Black Sea* that the Center for the Study of Democracy, Bulgaria implemented in cooperation with New Strategy Center, Romania. CSD appreciates the input received from multiple stakeholders and partners during a series of national and international meetings and events held in Sofia and online, and in particular the insights provided by Ms. Sarah Gamberini, Senior Policy Fellow, National Defence University, USA.

Authors:
**Dr Tatyana Novossiolova**, Senior Analyst, Center for the Study of Democracy
**Goran Georgiev**, Analyst, Center for the Study of Democracy




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 authors and do not necessarily reflect those of the United States Department of State.

Cover photo: Canva

**ISBN: 978-954-477-485-1**

# CONTENTS

# LIST OF FIGURES

# INTRODUCTION

Over the past decade, Bulgaria has been among the preferred targets of Russia's influence operations which employ **multifaceted and constantly evolving hybrid warfare** tactics. Such operations can be hard to detect and seek to undermine core democratic institutions and processes, deepen and exploit economic dependencies, and sow social divisions through deceit and manipulation. Russia has relied on **strategic corruption and regulatory manoeuvres** to capture key assets including in the energy and communications sectors and has leveraged deeply rooted sentiments on cultural and historical matters within society to advance its agenda by politicizing emotions along geopolitical lines. Because of their destabilizing effects, the Kremlin's influence operations pose a **significant threat to national security**. Such operations are not limited to a specific sector or area of activity. They span different domains combining hard, soft, and sharp power and relying on **proxies and trusted agents of influence**, which makes it difficult to distinguish between state and non-state actors, allowing denial of government involvement and evasion of responsibility.

Russia's **use of disinformation** is indicative in this regard, particularly as the Kremlin's disinformation campaigns are far-reaching, evolve quickly, and often amplify popular conspiracy theories. The Kremlin's disinformation machine has adapted rapidly to exploit topical issues and mass produce fake news and manipulated messaging in different languages. Online disinformation spreads within seconds and thanks to the social media can attract unprecedented number of readers and followers. Unauthentic behaviour on the internet through the use of 'troll farms', bots and other forms of automated interaction are important contributing factors to this trend, not least because strategy can significantly boost the popularity of specific disinformation narratives or make certain outlets or sources appear more authoritative than they are in reality. The Kremlin has integrated disinformation and diplomacy in ways that alter, augment, amplify and aggrandize its posture in the battlefield in Ukraine.

The Kremlin's readiness to **challenge chemical, biological, radiological, and nuclear (CBRN) security** through the deployment of hybrid warfare tactics signals an opportunistic strategy that disregards established international rules and norms. From multi-layered disinformation campaigns to the use of hard-to-detect toxic substances to eliminate opponents and perceived competitors, such subversive activities remain below the radar of openly declared aggression and can be hard to investigate. Because of their wide-ranging effects, CBRN-enabled hybrid threats put entire communities at risk, **sow fear** and bully vulnerable groups further into conspiracy pits. Inadvertent exposure to a toxic agent, mass panic, and **adoption of risk-prone behaviour** as a result of misleading messaging are a few examples of the implications that such threats can have at the societal level. Preventing, detecting, and responding to hybrid threats that involve materials and information associated with weapons of mass destruction (WMD) cut across multiple

sectors to ensure effective incident management and timely investigation, as well as to expose the perpetrators and bring them to justice.

As the ongoing war against Ukraine demonstrates, Russia's hybrid warfare strategy can escalate into a full-scale invasion. Long before the military attacks on Ukraine, the Kremlin has turned hybrid threats into its primary instruments of foreign policy. The covert annexation of Crimea and unfettered support for the separatist fighters in Donetsk and Luhansk regions that fuelled a protracted military conflict illustrate Russia's long-standing ambition to consolidate its **influence in the Black Sea region**. Against this backdrop, the decision to invade Ukraine signals the determination of the Russian leadership to use any means at its disposal to achieve their geopolitical goals and continue to project power. This has called on the most vulnerable countries like Bulgaria to quickly scramble resources to ramp up its infrastructure and capabilities for an effective response. The lead and support of NATO and EU partners, and in particular of the US has been of critical importance in building up and strengthening these capabilities with the aim of arriving at a **self-sustaining institutional response capacity**.

A robust strategy to prevent and counter Russia's hybrid campaigns requires concerted action on multiple fronts. An effective strategy against hybrid threats must address local vulnerabilities and focus on equipping government and civil society stakeholders with knowledge, techniques, and tools to mitigate the risk of malign foreign interference. This report outlines **a model of an integrated national approach** for preventing, detecting, and disrupting hybrid threats. The model centres on proactive deterrence, in order to ensure capacity for intercepting aggressive behaviour in a timely manner.

The proposed model approach features **four cross-cutting areas of action**:

(1) countering disinformation;

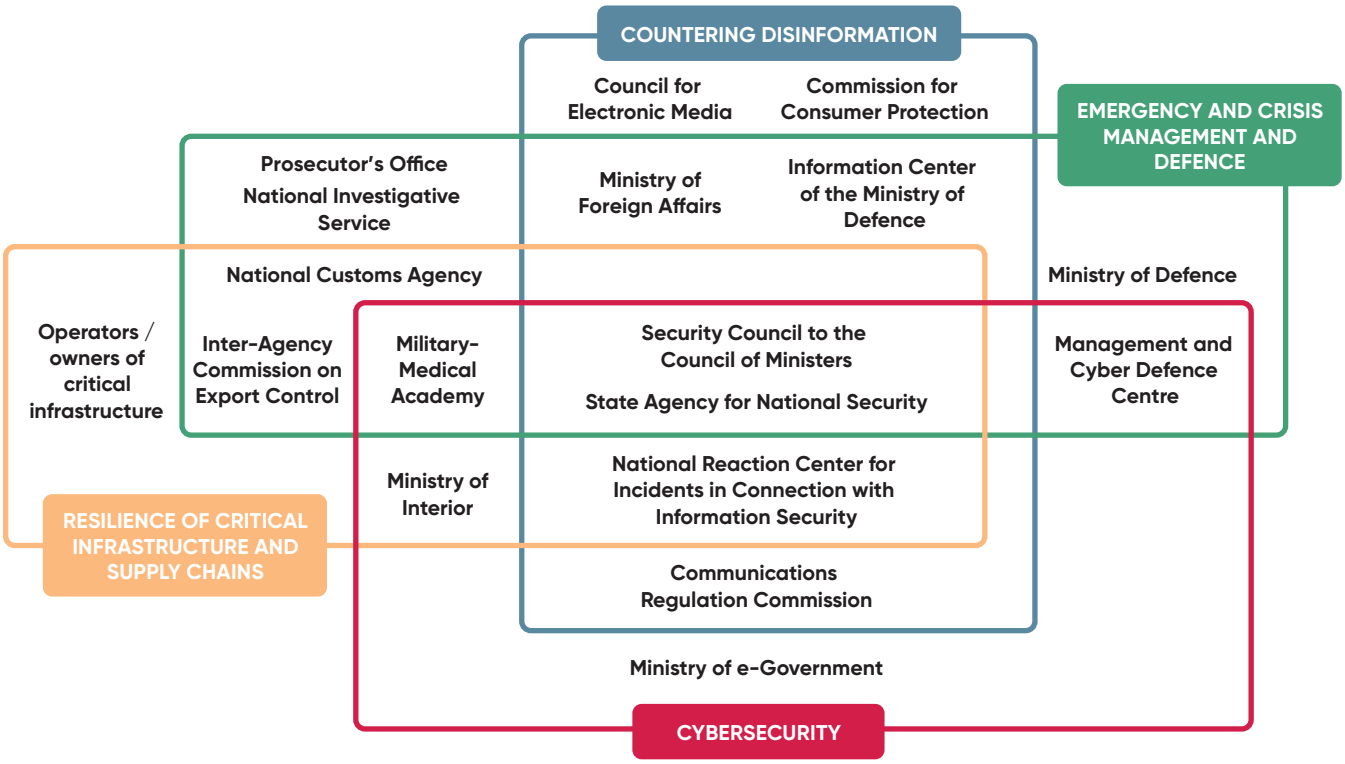
(2) cybersecurity;

(3) resilience of critical infrastructure and supply chains; and

(4) crisis and emergency management and defence.

The report further identifies and maps key competent authorities in Bulgaria that perform functions in these areas of action and relevant civil society-led initiatives (Figure 1). The **core elements of the national security system** in Bulgaria include competent authorities and structures performing diplomatic, defence-related, intelligence- and counter-intelligence-gathering, operative-searching, law enforcement, and security-related functions. These authorities are represented in the Security Council, which is a consultative and coordinating body to the Council of Ministers.

**Figure 1: Areas of Action and Key Competent Authorities in Bulgaria**




**Source:** CSD.

# AREAS OF ACTION

An integrated approach for combating hybrid threats at the national level requires a flexible combination of **vertical measures**, that is, top-down, or government initiatives, and bottom-up, or **civil society-led** initiatives, as well as **horizontal**, **cross-sectoral initiatives**. Any such package of measures must tackle vulnerabilities in depth and enable stakeholders to pre-empt influence operations. In particular, such measures must **strengthen national security and counter malign interference** in the political, economic, and socio-cultural domain. The proposed comprehensive approach focuses on **four primary areas of action**:

- Countering disinformation;
- Cybersecurity;
- Resilience of critical infrastructure and supply chains;
- Emergency and crisis management and defence.

The first two areas – **countering disinformation** and **cybersecurity** – impact all aspects of social life. Timely access to reliable information and safe and secure digital systems are underlying prerequisites for the provision of vital public and business services. Widely available accurate information and media transparency are also key to the functioning of democratic systems and processes.

**Critical infrastructure** encompasses entities that provide essential services in the sector of energy, transport, banking, financial market, health, drinking and waste water, digital infrastructure (e.g. providers of internet, cloud computing services, data centre services, electronic communications networks and services etc.), public administration, space, and production, processing, and distribution of food.[1] The **security of supply chains** must be approached from two perspectives. First, in the context of global trade, the efficient functioning of supply chains is indispensable to business continuity in critical sectors such as food production, health, and manufacturing. Disruption in the supply chains can result in delays and jeopardise communities' welfare. At the same time, economic dependencies can be exploited for gaining advantage in political matters, a tactic that the Kremlin has often used in the energy sector.[2] Second, the security of supply chains entails ensuring that international trade is not misused for illicit purposes, such as smuggling, trafficking, and sanction evasion.

---

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, 27 December 2022.

[2] See Stefanov, R. and Vladimirov, M. *The Kremlin Playbook in Southeast Europe: Economic Influence and Sharp Power*, 2020, Center for the Study of Democracy.

**Emergency and crisis management and defence** encompasses national capabilities and infrastructure for tackling threats to national security. Hybrid threats remain below the threshold of an armed attack but can take different forms including the use of unconventional weapons such as materials associated with chemical, biological, or nuclear weapons, collectively known as WMD. CBRN-enabled hybrid warfare resembles terrorism but unlike non-state actors who often have limited resources and expertise at their disposal, states like Russia are far more capable to orchestrate and conduct such activities frequently.

## Countering Disinformation

Disinformation campaigns are multi-faceted and can serve different purposes. Russia's disinformation strategy both relies on and aims at projecting economic influence. **Media capture** is at the heart of this strategy, whereby Kremlin-sponsored networks leverage regulatory, institutional, and procedural arrangements in target countries to infiltrate the media space, in order to seize control over public debates and political decision-making. Media capture encompasses **malign interference with business arrangements, ownership structures, and financial flows of media companies**, as well as with the content and editorial policies of media outlets and the overriding perceptions among managers, editors, and journalists.[3] This tactic enables the spread of disinformation narratives despite the sanctions against Russian media outlets that the EU has agreed after Russia's invasion of Ukraine.

Social media platforms constitute another avenue through which the Kremlin disseminates disinformation messaging. The Digital Services Act (DSA) and Digital Markets Act (DMA) which complement the European Commission's Code of Practice on Disinformation seek to enhance the **transparency of online platforms** and ensure that they are not misused for illegal or harmful purposes. The European Media Freedom Act further seeks to strengthen the elements of the Code of Practice that specifically deal with advertising, media monitoring, and the integrity of media services, including efforts to limit the access of malicious actors to advertising revenue and promote fact-checking and media literacy.[4] This Act also contains provisions for the transparency of media ownership and establishes a designated structure – the European Board for Media Services – which will promote the application of the rules and inform the development of guidelines on media regulatory matters.

Whilst Bulgaria is among the EU Member States that are most susceptible to Russian disinformation, **efforts to implement counter measures and build resilience remain patchy** and seem to lack overall coordination.

---

[3] 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.

[4] The European Parliament and the Council reached an agreement on the European Media Freedom Act in December 2023 and the final text of the regulation is subject to formal approval by April 2024. Once adopted, it will be binding and directly applicable in all Member States after 15 months.

The Council for Electronic Media, the national media supervisory body, and the Communications Regulation Commission which oversees electronic communications are the **regulators** that share duties as regards the implementation of EU sanctions against Russian media outlets. The Commission for Consumer Protection has responsibilities for the regulation of advertising services on online platforms and as such, plays a part in preventing websites that spread disinformation from generating advertising revenue.

The Council for Electronic Media is the competent authority that oversees the licensing of the electronic media service providers. As regards media content, the Council's activities are limited to specific functions, such as the supervision of service providers' compliance with the basic principles of freedom of expression, right to information, non-dissemination of content that inspires hatred or contradicts morality, compliance with copyrights, as well as journalist ethics. The publicly owned and funded national electronic broadcasters, the Bulgarian National Television and the Bulgarian National Radio, and the national news-wire service, BTA play an important role in promoting the adoption of good practices for public engagement such as setting up fact-checking portals and media literacy programmes to enhance the resilience of the country's information space against the spread of manipulative and misleading content.

The State Agency for National Security (SANS) plays a key role in tackling foreign information operations in Bulgaria. The Agency is the lead authority that detects and investigates foreign special services' activities against Bulgaria. The General Directorate for Combating Organised Crime of the Ministry of Interior is responsible for preventing the spread of illegal content online, including content that propagates or incites discrimination, hatred, or violence based on race, ethnicity, or nationality.

The Council of Ministers, the Ministry of Foreign Affairs and the Ministry of Defence lead Bulgaria's policy efforts to build up **strategic communications** capabilities. As part of its strategic communications portfolio of initiatives, the **Information Centre of the Ministry of Defence** administers a Disinformation Radar, a publicly available up-to-date fact-checking platform that debunks popular pro-Kremlin disinformation narratives on different topics. Whilst mainly focused on defence-related issues, the platform also seeks to flag misleading and manipulative messaging on everyday matters that are likely to attract wide public interest.

There are multiple efforts to enhance resilience against disinformation at the grassroots level in Bulgaria. **Civil society and the business community** remain the most active stakeholders in media monitoring and exposing disinformation campaigns. Despite increasing efforts at promoting, media literacy, these activities have not become part of formal educational curricula, yet, which significantly limits their overall reach and impact.

## Cybersecurity

Cyber-attacks are on the rise and geopolitics, particularly Russia's ongoing war against Ukraine remains an important factor that shapes the cybersecurity landscape in the EU. A case in point is the **growth of hacktivism** – hacker attacks for political or social causes – as a result of the spread of manipulative messaging and disinformation by Kremlin-backed and pro-Kremlin sources. State-sponsored **malign cyber activities** have also tried to hide under the flag of hacktivism, as evidenced by the pro-Russian group, *Killnet*.[5]

**Cyber espionage** is another preferred tactic in Russia's arsenal of cyber malicious activities. The Russian technology industry plays a critical part in supporting Kremlin's offensive cyberwarfare capabilities. Cyber espionage operations have also benefited from the misuse of legitimate tools that allow intruders to evade detection over an extended period of time. About half of the attacks that occurred between January 2022 and August 2023 targeted the government administration sector.[6] About 66 per cent of the attacks were motivated by political reasons or activist agendas and 50 per cent of the global incidents were linked to Russia's war against Ukraine.

To harmonise and bolster cybersecurity efforts across European Union Member States and achieve a high common level of cybersecurity, the European Commission has advanced a framework for risk management at critical entities, both public and private.[7] The EC provisions apply to **high criticality sectors** which include all critical infrastructure sectors. It also applies to entities in other critical sectors such as postal and courier services, waste management, manufacturing, production, and distribution of chemicals, manufacturing (e.g. medical and diagnostic devices, electrical equipment, computer, optical, and electronic products, motor vehicles, etc.), digital service providers, and research.

Two additional pieces of **cybersecurity legislation** are currently being considered at the **EU level**. The Cyber Solidarity Act seeks to strengthen detection, preparedness, and response capacities for addressing cybersecurity threats and attacks. This Act envisages the creation of a network of security operations centres (European Cybersecurity Shield) and Cyber Emergency Mechanism that will offer, among other things, the provision of assistance by one Member State to another in case of a cyber-incident. The Cyber Resilience Act aims to introduce new rules on the development of products or software with a digital component, in order to reduce cybersecurity vulnerabilities. This framework features cybersecurity requirements for the planning, design, development, and maintenance of regulated products and an obligation to provide a duty of care for the entire lifecycle of such products.

---

5 ENISA, *ENISA Threat Landscape Report 2023*, 19 October 2023. Killnet has repeatedly carried out cyber-attacks against Bulgarian public administration, critical infrastructure, and even civil society organisations, including the Center for the Study of Democracy.

6 ENISA, *ENISA Threat Landscape for DoS Attacks – 2023*, 19 October 2023.

7 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 2022.

The **national framework for cybersecurity** in Bulgaria features **three pillars**:

- network and information security;
- cyber defence; and
- combating cybercrime.

The Ministry of e-Government is the leading **government authority** in the area of network and information security. It also hosts the National Reaction Center for Incidents in Connection with Information Security (CERT Bulgaria) that is responsible for activities in four domains, namely emergency warning, vulnerability management, security incident management, and artefact management during the investigation of cyber incidents. SANS supports the efforts to ensure cyber defence, particularly as regards the threat assessment, identification, detection, and management of hybrid attacks in cyberspace. Such attacks can take different forms and pursue various objectives ranging from sabotage to data theft and permanent system damage. The Management and Cyber Defence Centre at the Ministry of Defence is a capacity building facility that provides training and human resource development programmes to counter cyber-attacks and enhance prevention. The Cybercrime Unit of the General Directorate for Combating Organised Crime at the Ministry of Interior coordinates the prevention and investigation of illegal activities in cyberspace, including ransomware, phishing, DoS, and other forms of hacker attacks, online financial crime and fraud, and copyright infringement.

At the **grassroots level**, the Cybersecurity Laboratory at Sofia Tech Park is a leading provider of analytical and applied services for enhancing institutional cybersecurity and promoting human resource development for business and public sector.

## Resilience of Critical Infrastructure and Supply Chains

Prior to the war against Ukraine, pro-Russian groups carried out cyber-attacks against the Ukrainian power grid system, as a result of which several hundred thousand local citizens were deprived of vital services. Following the invasion of Ukraine, Russian forces have **systematically targeted local critical infrastructure**. The continuing occupation of the Zaporizhzhia Nuclear Power Plant, the bombing of the Nova Kakhovka dam, and frequent attacks against hospitals, water, power, and food storage and supply systems, and transport infrastructure are indicative of the scale of hostilities. Russia's belligerent activities also pose a grave danger to **maritime safety and security in the Black and Azov Sea** and limit the capacity of Ukraine to use the Black Sea trade routes. A case in point is the collapse of the grain deal after Russia unilaterally refused to renew its mandate in the summer of 2023.

EU regulations require Member States to **carry out risk assessment** that take into account the risk of hybrid or other antagonistic threats, in order to designate critical entities in sectors that provide essential services for

the functioning of societies.[8] Any entity that is identified as a critical entity must be notified accordingly and conduct a regular risk assessment at least every four years, if not otherwise required under national regulations. Critical entities must have in place internal protocols and procedures for managing security risks, both physical and cyber, and for recovery in case of a security incident. Such measures also include background checks of individuals who perform or apply for sensitive roles within critical entities or have access to the premises, or the information or control systems of such entities.

The EU **Economic Security** Strategy adopted in 2023 identifies four sets of interconnected risks that require urgent action to guarantee the resilience of physical and cyber properties of critical infrastructure and supply chains, mitigate the risk of economic coercion, and prevent security technology leakage. The Strategy features a broad package of measures that seek to strengthen the mechanisms for screening of foreign direct investment; counter foreign malign interference in research and innovation; and enhance the effectiveness of export controls on dual-use items and strategic trade controls to prevent the misuse of technological advances for purposes that threaten EU security and stability. The EU has also ramped up its efforts on the protection of the Union and its Member States from **economic coercion by third countries**.[9] The EU has established a legal framework for deterring and tackling the misuse of economic relations such as trade or investment, in order to affect the position or actions of the EU or a Member State.

Under the existing rules in Bulgaria, the government is responsible for identifying and designating entities as **national critical infrastructure**. Competent authorities, i.e. ministries or other branches of the executive are responsible for identifying critical infrastructure in their respective sector. As part of this procedure, each authority must set up a permanent working group which develops criteria and a preliminary list of potential critical entities. The Minister of Interior provides guidance on the methodology for risk assessment and the working groups within the respective competent authorities develop and provide the methodology to the owners/operators of critical infrastructures. The protection of critical infrastructure is a key objective of the national security system and several authorities, most notably, SANS has a mandate to protect the country's critical infrastructure and assets.

The **owners/operators** of critical infrastructures are the individuals or legal entities that are responsible for investing in or for ensuring the normal functioning, sustainability and integrity of a system or part of a system identified as critical infrastructure. The screening of investments in critical infrastructure is assigned to the competent authority authorised to administer the respective critical infrastructure sector (e.g. the systems for generation and transmission of electricity fall into the sector of energy and are administered

---

[8] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, 2022.

[9] Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries, 2023.

by the Ministry of Energy). In 2024, the Bulgarian Parliament is expected to adopt a bill introducing a **national investment screening mechanism**.[10]

The Interagency Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction within the Ministry of Economy oversees the export, import, transfer, transit, and brokerage of **defence-related products and dual-use items and technologies**. The National Customs Agency performs control functions for preventing the illicit trafficking of strategic goods, including dual-use items and technologies.

## Emergency and Crisis Management and Defence

Russia's renewed interest in the use of WMD poses significant risks to EU security. The spectrum of WMD hybrid threats is wide-ranging. In the recent years, Russian security services have carried out several **targeted assassination attacks** using toxic chemical, biological, and radioactive agents. On at least two occasions, Russian operatives deployed "Novichok" nerve agent with one of these attacks resulting in the poisoning of several individuals, loss of life, and significant decontamination costs.

The Russian government, state-controlled media, and pro-Kremlin media outlets have actively disseminated disinformation narratives accusing neighbouring countries, including Georgia and Ukraine of developing biological weapons in an attempt to **undermine international cooperation** in the area of health and disease prevention. From the outset of the invasion against Ukraine, the Russian nuclear forces were put on higher alert and the Kremlin has repeatedly referred to its nuclear posture, including by taking the decision to deploy nuclear weapons in Belarus.

Most recently, several reports have indicated that the Russian troops are deploying tear gas against the Ukrainian army. Tear gas belongs to the group of riot control agents (RCA) and international law prohibits the use of RCAs as a means of warfare.

NATO's Chemical, Biological, Radiological, and Nuclear (CBRN) Defence Policy is comprehensive and provides a framework for strengthening the **CBRN defence capabilities** and resilience of NATO Member States against the full spectrum of CBRN and WMD threats.[11] The Policy calls for greater and more effective civil-military interaction and underlines the importance of scientific and technical collaboration and strategic communication and public diplomacy.

The Security Council to the Council of Ministers in Bulgaria is a key decision-making mechanism which develops and puts forward concrete steps and measures for risk and crisis management and threat reduction; facilitates multi-agency coordination; and supports crisis communication. It has a leading role in crisis management and its secretariat fulfils the functions of a National Situation Centre.

---

[10] *Investment Screening for Enhanced Economic Security*, Policy Brief No 142, December 2023, Center for the Study of Democracy.

[11] NATO's Chemical, Biological, Radiological and Nuclear (CBRN) Defence Policy, 14 June 2022.

The Ministry of Defence is the leading national authority for WMD and CBRN defence. The Bulgarian Army operates an **automated information system for surveillance and early warning** in case of CBRN threats. This system is connected with the National Operation-Communication-Information Centre of the General Directorate Fire Safety and Civil Protection of the Ministry of Interior and facilitates data sharing with the counterpart systems of NATO Member States. The Military-Medical Academy under the auspices of the Ministry of Defence is an integral element of the national infrastructure for managing the consequences of military conflict, natural disasters, industrial accidents, and terrorist attacks. The Academy also provides continued professional training in key fields such as healthcare provision in case of exposure to radiation and toxic poisoning. The State Agency for National Security (SANS) performs the functions of a **National Coordination Centre for Counter-Proliferation** which coordinates inter-agency and multi-stakeholder cooperation in the area of national security and countering WMD threats.

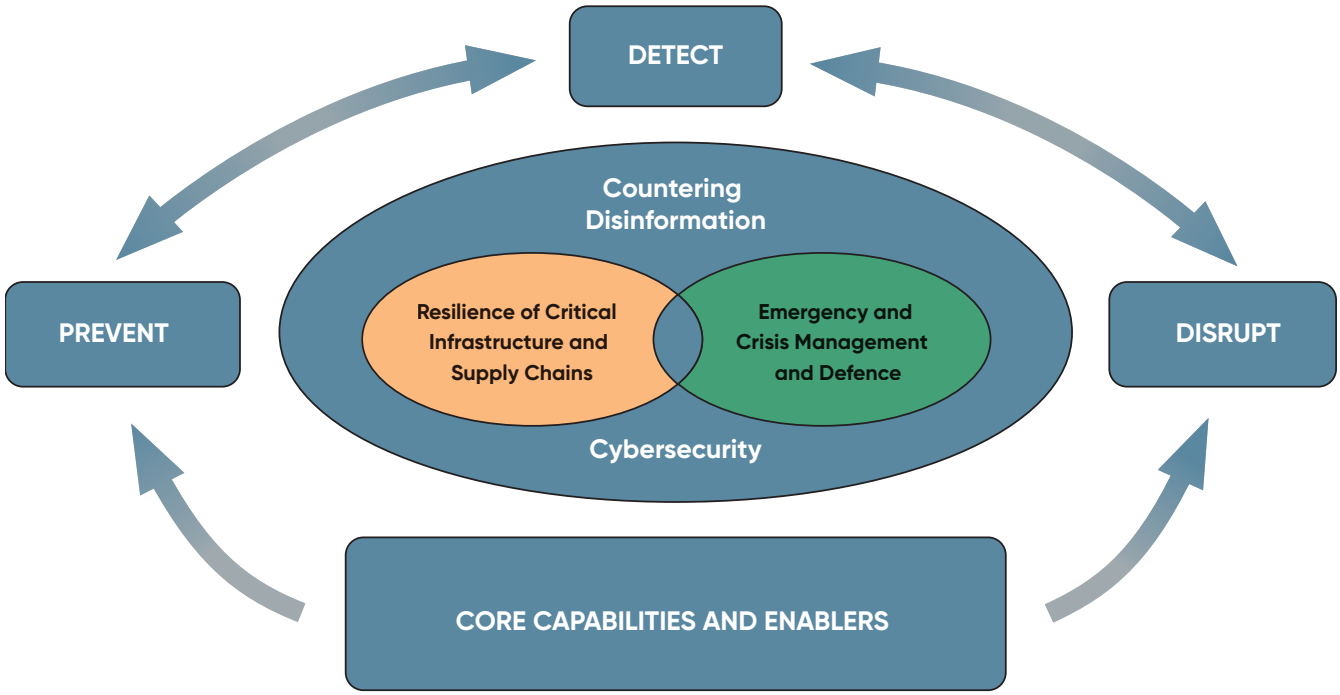
The NATO Crisis Management and Disaster Response Centre of Excellence (CMDR COE) situated in Bulgaria offers continued professional development courses for enhancing operational capacity for emergency preparedness and response to current and emerging security threats.

The law enforcement sector including the Ministry of Interior and National Investigative Service, as well as the Prosecutor's Office play a leading role in the investigation of CBRN-enabled criminal acts such as targeted assassination attacks involving chemical, biological, or radiological materials or agents.

# STRATEGIC OBJECTIVES AND NEXT STEPS

The **model national approach** for countering hybrid threats that centres on proactive deterrence must integrate at least **three strategic objectives**: (1) prevent, (2) detect, and (3) disrupt (Figure 2). Fulfilling these objectives requires concerted efforts across all four areas of action and the active involvement of government and civil society stakeholders in addressing the risk of malign interference. It is essential that appropriate policies and measures are in place to mitigate the negative impacts of hybrid warfare and facilitate a quick recovery in case of an incident. A multi-layered national system that seeks to limit the potential for malign interference can serve as a deterrence against malicious actors.

**Figure 2: Elements of an Integrated Approach for Countering Hybrid Threats**




**Source:** CSD.

Achieving each of the three strategic objectives requires **a set of corresponding core capabilities** and enablers that facilitate the process of maintaining the core capabilities:

- To **prevent** hybrid threats, Bulgaria must ensure the following **core capabilities**:
  - o intelligence gathering for monitoring of the threat landscape and rapid identification of national security concerns related to foreign malign interference;

- inter-agency coordination and data sharing among competent authorities and stakeholders that promotes a shared understanding of hybrid threats and how they can manifest;
- defence planning that takes into account the spectrum of hybrid threats and drives the acquisition of appropriate operational and technical capacities across sectors;
- strategic communications that tackle the risk of foreign information manipulation operations and disinformation campaigns;
- threat awareness and media literacy at the societal level that enhances sensitivity toward foreign malign interference, including disinformation.

Key **enablers** that contribute to the sustainability of these capabilities include: (1) implementation of intelligence, surveillance, and reconnaissance systems through strategic engagement with EU and NATO partners; (2) policy and regulatory measures that ensure the transparency of foreign investment, procurement, and political party financing; (3) enforcement of legal and procedural frameworks for combating corruption, money laundering, and sanction evasion across sectors; (4) standardisation and licensing of activities related to the operation and maintenance of critical entities; (5) regulatory and institutional arrangements regarding the ownership and funding of media.

- To **detect** hybrid threats, Bulgaria must have in place the following **core capabilities**:
  - nation-wide system for early warning;
  - periodic review of the implementation of policies, regulations, and protocols for tackling hybrid threats to ensure that the relevant measures and initiatives are up-to-date;
  - electronic record system documenting examples of past hybrid warfare attacks to support the investigation of suspicious activities.

Key **enablers** that contribute to the sustainability of these capabilities include: (1) institutional and sector-wide mechanisms for reporting suspicious activities related to foreign malign interference; (2) integrated national mechanism for cross-sectoral vulnerability assessment; (3) incentives for stakeholders to promote security-relevant practices and behaviours to counter foreign malign interference.

- To **disrupt** hybrid threats, Bulgaria must ensure the following **core capabilities**:
  - resourced inter-agency teams and units for rapid response in case of a hybrid attack;
  - risk communication, messaging, and counter-messaging in case of hybrid warfare;
  - mechanisms for international assistance and cooperation in case of hybrid warfare.

Key **enablers** that contribute to the sustainability of these capabilities include: (1) crisis management strategy that focuses on intercepting foreign adversarial activities; (2) investigation, exposure, and prosecution of activities related to foreign malign interference; (3) cross-sectoral initiatives to counter disinformation in the media and cyber space.