ЦЕНТЪР ЗА ИЗСЛЕДВАНЕ НА ДЕМОКРАЦИЯТА

Противодействие на хибридната война в България

Стратегическа оценка на националните способности и инфраструктура

Противодействие на хибридната война в България

Стратегическа оценка на националните способности и инфраструктура

ЦЕНТЪР ЗА
ИЗСЛЕДВАНЕ НА
ДЕМОКРАЦИЯТА

България е сред предпочитаните цели на руските операции за влияние, които използват тактиката на хибридната война, като съчетават твърда, мека и остра сила. Настоящият доклад очертава модел на интегриран национален подход за превенция, разкриване и предотвратяване на хибридните заплахи. Моделът се основава върху мерките на проактивното възпиране, за да се осигури капацитет за своевременното предотвратяване на намеса. Докладът разглежда основните компетентни органи и набор от граждански инициативи в България в четири взаимосвързани области на действие: противодействие на дезинформацията; киберсигурност; устойчивост на критичната инфраструктура и веригите за доставки; отбрана и управление на извънредни ситуации и кризи.

Разработването на този доклад е част от инициативата „Противодействие на хибридните заплахи от неконвенционални оръжия в Черноморския регион“, която Центърът за изследване на демокрацията, България, реализира в сътрудничество с Центъра за нови стратегии, Румъния. Центърът за изследване на демокрацията оценява приноса на експертите и партньорите, взели участие в проведените национални и международни срещи и събития, и изразява признателност към г-жа Сара Гамберини, старши сътрудник в Националния университет по отбрана на САЩ за споделените идеи и възгледи.

Автори:
Д-р Татяна Новосьолова, старши анализатор, Център за изследване на демокрацията
Горан Георгиев, анализатор, Център за изследване на демокрацията

Тази публикация е финансирана от Държавния департамент на САЩ. Съдържанието ѝ представя гледната точка на нейните автори, които единствени носят отговорност за нея.

Снимка на корицата: Canva

ISBN: 978-954-477-484-4

СЪДЪРЖАНИЕ

СПИСЪК НА ФИГУРИТЕ

ВЪВЕДЕНИЕ

През последното десетилетие България е сред предпочитаните цели на руските операции за влияние, които използват **многостранни и постоянно развиващи се** тактики на **хибридна война**. Подобни операции могат да бъдат трудни за разпознаване и целят подкопаването на основните демократични институции и процеси, задълбочаването и използването на икономическите зависимости за политически цели и насаждането на социално разделение чрез измама и манипулация. Русия разчита на **стратегическа корупция и регулаторни маневри**, за да завладее ключови активи, включително в сферата на енергетиката и комуникациите, и използва обществените нагласи и настроения по културни и исторически въпроси, за да постигне целите си, като политизира емоциите въз основа на геополитическо противопоставяне. Операциите на Кремъл за оказване на влияние представляват **съществена заплаха за националната сигурност**, най-вече заради своите дестабилизиращи ефекти. Тези операции не са ограничени до конкретен сектор или сфера на дейност. Те обхващат различни области, като съчетават твърда, мека и остра сила и разчитат на **мрежи от агенти за влияние**, което затруднява разграничаването на държавните от недържавните участници. Това позволява на руското ръководство да отрече своето участие в провеждането на „активни мероприятия“ и да попречи на установяването на отговорност.

Използването на дезинформация от страна на Русия е показателно в това отношение. Кампаниите за дезинформация на Кремъл са широкообхватни, разгръщат се и се променят бързо и често се възползват от популярните конспиративни теории, като целенасочено засилват тяхното въздействие. Пропагандната машината на Кремъл се адаптира бързо, което ѝ позволява да произвежда огромно количество фалшиви новини и подвеждащо съдържание по актуални теми на различни езици. В интернет пространството дезинформацията се разпространява за секунди и благодарение на социалните медии може да привлече безпрецедентен брой читатели и последователи. Неавтентичното поведение в интернет чрез използването на „ферми за тролове“, автоматизирани техники на основата на изкуствен интелект (ботове) и други форми на автоматизирано взаимодействие са важни фактори, които допринасят за тази тенденция. Например системното прилагане на подобни тактики може значително да увеличи популярността на конкретни дезинформационни наративи или да накара определени медии или източници да изглеждат по-авторитетни, отколкото са в действителност. Кремъл интегрира дезинформацията и дипломацията, с цел да промени, подсили, утвърди и спечели подкрепа за позициите си на бойното поле в Украйна.

Готовността на Кремъл да **подкопае химическата, биологичната, радиационната и ядрената (ХБРЯ) сигурност** чрез използването на тактики за хибридна война е сигнал за опортюнистична стратегия, която не зачита установените международни правила и норми. От многопластовите кампании за дезинформация до използването на трудни за идентифициране токсични вещества в държавно-спонсорирани покушения, по-

добни подривни дейности остават под прага на действителен въоръжен конфликт, а техните извършители невинаги е възможно да бъдат подведени под наказателна отговорност. Хибридните заплахи, които използват ХБРЯ материали или свързаната с тях информация, имат широкообхватно въздействие и излагат на риск цели общности, **сеят страх** и засилват популярността на конспиративните теории. Подобни заплахи могат да имат сериозни последици на обществено равнище, като това включва възможното излагане на токсичен агент и заразяване, масовата паника и **възприемането на рисково поведение** на базата на подвеждащо съдържание и послания. Превенцията, откриването и предотвратяването на хибридните заплахи, свързани с оръжията за масово унищожение (ОМУ), обхващат множество сектори, като целта е да се осигури ефективното управление на подобни инциденти и тяхното своевременно разследване и разкриване.

Както показва продължаващата война срещу Украйна, руската стратегия за хибридна война може да прерасне в пълномащабна инвазия. Много преди военните атаки срещу Украйна, Кремъл превърна хибридните заплахи в свой основен инструмент на външната си политика. Анексирането на Крим и неограничената подкрепа за сепаратистките бойци в Донецка и Луганска област, които допринесоха за разпалването на продължителен военен конфликт, са показателни за отдавнашната амбиция на Русия да затвърди **влиянието си в Черноморския регион**. На този фон, решението за въоръжен конфликт с Украйна е сигнал за решимостта на руското ръководство да използва всички налични средства, за да постигне геополитическите си цели и да си осигури стратегическо надмощие. Агресивният подход на Кремъл наложи най-уязвимите държави като България бързо да мобилизират ресурси за подсилване на инфраструктурата и способностите си за ефективен отговор. Водещата роля и подкрепата на партньорите от НАТО и ЕС, и по-специално на САЩ, бяха от решаващо значение за изграждането и укрепването на тези способности с цел постигане на **самостоятелен институционален капацитет за реагиране**.

Интегрираният подход за предотвратяване и противодействие на хибридните кампании на Русия изисква координирани действия на няколко фронта. За да е максимално ефективна, стратегията срещу хибридните заплахи следва да е насочена, преди всичко, към преодоляването на уязвимостите на местно равнище и да се фокусира върху обезпечаването на заинтересованите страни от правителството и гражданското общество с ресурси, техники и инструменти за намаляване на риска от чуждестранна намеса. Настоящият доклад очертава **модел на интегриран национален подход** за превенцията, разкриването и предотвратяването на хибридните заплахи. Моделът е съсредоточен върху проактивното възпиране, за да се осигури капацитет за своевременно предотвратяване на чужда намеса.

Предложеният подход включва **четири хоризонтални области на действие**:

- Противодействие на дезинформацията
- Киберсигурност
- Устойчивост на критичната инфраструктура и веригите за доставки
- Отбрана и управление на кризи и извънредни ситуации.

Докладът разглежда основните компетентни органи в България, които изпълняват функции в тези области на действие, както и релевантни инициативи на гражданското общество (Фигура 1). **Основните елементи на системата за национална сигурност** в България включват компетентни органи и структури, които изпълняват функции в сферата на дипломацията, отбраната, събирането на разузнавателна и контраразузнавателна информация, оперативно-издирвателна дейност, правоприлагане и сигурност. Тези органи са представени в Съвета по сигурността, който е консултативен и координиращ орган към Министерския съвет.

Фигура 1: Области на действие и ключови компетентни органи в България

Източник: Център за изследване на демокрацията.

ОБЛАСТИ НА ДЕЙСТВИЕ

Интегрираният подход за борба с хибридните заплахи на национално равнище изисква гъвкава комбинация от **вертикални мерки**, т.е. инициативи от горе надолу или правителствени инициативи, и инициативи от долу нагоре или **инициативи, ръководени от гражданското общество**, както и **хоризонтални, междусекторни инициативи**. Всеки такъв пакет от мерки трябва да се занимава с уязвимостите в дълбочина и да дава възможност на заинтересованите страни да изпреварват операциите за оказване на влияние. По-специално, тези мерки трябва да **укрепват националната сигурност и да противодействат на злонамерената намеса** в политическата, икономическата и социално-културната област. Предложеният всеобхватен подход се съсредоточава върху **четири основни области на действие**:

- Противодействие на дезинформацията
- Киберсигурност
- Устойчивост на критичната инфраструктура и веригите за доставки
- Отбрана и управление на извънредни ситуации и кризи.

Първите две области – противодействие на **дезинформацията** и **киберсигурност –** оказват влияние върху всички аспекти на социалния живот. Навременният достъп до надеждна информация и безопасните и сигурни цифрови системи са основни предпоставки за предоставянето на жизненоважни обществени и бизнес услуги. Широко достъпната точна информация и прозрачността на медиите също са от ключово значение за функционирането на демократичните системи и процеси.

Критичната инфраструктура обхваща субекти, които предоставят основни услуги в областта на енергетиката, транспорта, банковото дело, финансовия пазар, здравеопазването, питейните и отпадъчните води, цифровата инфраструктура (напр. доставчици на интернет, изчислителни услуги в облак, услуги на центрове за данни, електронни съобщителни мрежи и услуги и т.н.), публичната администрация, космическото пространство и производството, преработката и дистрибуцията на храни.[1] **Сигурността на веригите за доставки** трябва да се разглежда от две гледни точки. Първо, в контекста на световната търговия ефективното функциониране на веригите за доставки е необходимо за непрекъснатостта на бизнеса в критични сектори като производството на храни, здравеопазването и производството. Прекъсването на веригите за доставки може да доведе до закъснения и да застраши благосъстоянието на общностите. В същото време икономическите зависимости могат да бъдат използвани

[1] Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. относно устойчивостта на критичните обекти и за отмяна на Директива 2008/114/ЕО на Съвета, 27 декември 2022 г.

за получаване на предимство в политически план – тактика, която Кремъл често използва в енергийния сектор.[2] На второ място, сигурността на веригите за доставки предполага да се гарантира, че международната търговия не се използва за незаконни цели, като контрабанда, трафик и избягване на санкции.

Отбрана и управление на извънредни ситуации и кризи обхваща националните способности и инфраструктура за справяне със заплахите за националната сигурност. Хибридните заплахи остават под прага на въоръжено нападение, но могат да приемат различни форми, включително използването на неконвенционални оръжия, като например материали, свързани с химически, биологични или ядрени оръжия, известни под общото наименование ОМУ. Хибридната война със използване на ХБРЯ материали наподобява тероризма, но за разлика от недържавните участници, които често разполагат с ограничени ресурси и експертен опит, държави като Русия са много по-способни да организират и провеждат често такива дейности.

Противодействие на дезинформацията

Кампаниите за дезинформация са многостранни и могат да имат различни цели. Стратегията на Русия за дезинформация разчита на икономическо влияние и има за цел да го проектира. **Завладяването на медиите** е в основата на тази стратегия, при която спонсорираните от Кремъл мрежи използват регулаторни, институционални и процедурни механизми в целевите държави, за да проникнат в медийното пространство и да установят контрол върху обществените дебати и вземането на политически решения. Завладяването на медиите включва **злонамерена намеса** в бизнес договореностите, структурите на собственост и финансовите потоци на медийните компании, както и в съдържанието и редакционните политики на медиите и преобладаващите възприятия сред мениджърите, редакторите и журналистите.[3] Тази тактика дава възможност за разпространение на дезинформационни наративи въпреки санкциите срещу руските медии, които ЕС договори след нахлуването на Русия в Украйна.

Платформите на социалните медии представляват друг канал, чрез който Кремъл разпространява дезинформационни съобщения. Регламентът за цифровите услуги и Регламентът за цифровите пазари, които допълват Кодекса на практиките на Европейската комисия относно дезинформацията, имат за цел да повишат **прозрачността на онлайн платформите** и да гарантират, че с тях не се злоупотребява за незаконни или вредни цели. Европейският законодателен акт за свободата на медиите има за цел освен това да укрепи елементите на Кодекса относно дезинформацията, които се отнасят конкретно до рекламата, медийния мониторинг и интегритета на медийните услуги, включително усилията за ограничаване на достъпа на злонамерени участници до приходите от реклама

---

[2] Вж. Стефанов, Р. и Владимиров, М. Кремълският наръчник в Югоизточна Европа: Икономическо влияние и остра сила, София: Център за изследване на демокрацията, 2020.

[3] Георгиев, Г., Петрова, В., и Цабала, К., Разбиване на кода: Руска и китайска дезинформация и незаконни финансови потоци в Югоизточна Европа, София: Център за изследване на демокрацията, 2023.

и насърчаване на проверката на фактите и медийната грамотност.[4] Този законодателен акт съдържа също така разпоредби за прозрачност на собствеността на медиите и – урежда създаването на Европейски съвет за медийни услуги, който ще насърчава прилагането на правилата и ще предоставя информация за разработването на насоки по въпросите на медийното регулиране.

Макар че България е сред държавите – членки на ЕС, които са най-податливи на руска дезинформация, **усилията за прилагане на мерки за противодействие и изграждане на устойчивост остават разпокъсани** и без цялостна координация.

Съветът за електронни медии, националният орган за медиен надзор, и Комисията за регулиране на съобщенията, в чиито правомощия е контролът на електронните съобщения, са **регулаторните органи**, които си поделят задълженията по отношение на прилагането на санкциите на ЕС срещу руските медии. Комисията за защита на потребителите има отговорности за регулирането на рекламните услуги в онлайн платформите и в тази връзка играе роля в предотвратяването на генерирането на рекламни приходи от уебсайтове, които разпространяват дезинформация.

Съветът за електронни медии е компетентният орган, който следи за лицензирането на доставчиците на електронни медийни услуги. Що се отнася до медийното съдържание, дейността на Съвета е ограничена до специфични функции, като например надзор върху спазването от страна на доставчиците на услуги на основните принципи на свободата на изразяване, правото на информация, неразпространението на съдържание, което внушава омраза или противоречи на морала, спазването на авторските права, както и на журналистическата етика. Националните електронни радио- и телевизионни оператори, които са публична собственост и се финансират от държавата – Българската национална телевизия и Българското национално радио, както и Българската телеграфна агенция (БТА), играят важна роля в насърчаването на възприемането на добри практики за обществена ангажираност, като например създаването на портали за проверка на фактите и програми за медийна грамотност, за да се повиши устойчивостта на информационното пространство в страната срещу разпространението на манипулативно и подвеждащо съдържание.

Държавната агенция „Национална сигурност“ (ДАНС) играе ключова роля в противодействието на чуждестранните информационни операции в България. Агенцията е водещият орган, който разкрива и разследва дейността на чужди специални служби срещу България. Главна дирекция „Борба с организираната престъпност“ (ГДБОП) към Министерството на вътрешните работи отговаря за предотвратяване на разпространението на незаконно съдържание в интернет пространството, включително съдържание, което разпространява или подбужда към дискриминация, омраза или насилие, основани на раса, етническа принадлежност или националност.

---

[4] През декември 2023 г. Европейският парламент и Съветът постигнаха споразумение по Европейския законодателен акт за свободата на медиите, а окончателният му текст подлежи на официално одобрение до април 2024 г. След като бъде приет, той ще стане задължителен и пряко приложим във всички държави членки след 15 месеца.

Министерският съвет, Министерството на външните работи и Министерството на отбраната изпълняват ключова роля в изграждането на способности за **стратегически комуникации**. Като част от портфолиото си от инициативи в тази област, **Информационният център на Министерството на отбраната** администрира Дезинформационен радар – публично достъпна платформа за проверка на факти, която оборва популярни прокремълски дезинформационни наративи по актуални теми. Макар да е насочена основно към въпроси, свързани с отбраната, платформата се стреми да сигнализира и за подвеждащо и манипулативно съдържание, което представлява широк обществен интерес.

В България се полагат многобройни усилия за повишаване на устойчивостта срещу дезинформацията на местно равнище. **Гражданското общество и бизнесът** продължават да бъдат най-активните участници в медийния мониторинг и разкриването на кампании за дезинформация. Въпреки нарастващите усилия за насърчаване на медийната грамотност, тези дейности все още не са част от официалните образователни програми, което значително ограничава цялостния им обхват и въздействие.

Киберсигурност

Кибератаките се увеличават, а геополитиката, особено продължаващата война на Русия срещу Украйна, остава важен фактор, който определя средата за киберсигурност в ЕС. Пример за това е **ръстът на „хактивизма“** – хакерски атаки за политически или социални каузи – в резултат на разпространението на манипулативни съобщения и дезинформация от подкрепяни от Кремъл и прокремълски източници. Държавно-спонсорирани **злонамерени дейности в киберпространството** също често се представят за хактивизъм, за което свидетелства проруската група *Killnet*.[5]

Кибершпионажът е друга предпочитана тактика в арсенала от киберзлоупотреби на Русия. Руската технологична индустрия играе важна роля в подпомагането на офанзивните способности на Кремъл за водене на кибервойна. Операциите за кибершпионаж се възползват и от злоупотребата с легитимни инструменти, което позволява на нарушителите да избегнат откриване за продължителен период от време. Около половината от атаките за отказ на услуга, извършени между януари 2022 г. и август 2023 г., са насочени към сектора на държавната администрация.[6] Около 66% от тези атаки са били мотивирани от политически причини или активистки програми, а 50% от глобалните инциденти са били свързани с войната на Русия срещу Украйна.

За да хармонизира и укрепи усилията за киберсигурност в държавите – членки на Европейския съюз, и да постигне високо общо ниво на киберсигурност, Европейската комисия разработи рамка за управление на

[5] ENISA, *ENISA Threat Landscape Report 2023*, 19 октомври 2023 г. Killnet многократно е извършвал кибератаки срещу българската публична администрация, критичната инфраструктура и дори срещу организации на гражданското общество, включително срещу Центъра за изследване на демокрацията.

[6] ENISA, *ENISA Threat Landscape for DoS Attacks – 2023*, 19 октомври 2023 г.

риска в критични структури – както публични, така и частни.[7] Разпоредбите на ЕК са приложими в **сектори с обществена и стратегическа значимост**, каквито са всички сектори на критичната инфраструктура. Прилагат се и за субекти в други обществено значими сектори, като пощенските и куриерските услуги, управлението на отпадъци, химическата промишленост, производството (например медицински и диагностични уреди, електрическо оборудване, компютърни, оптични и електронни продукти, моторни превозни средства и т.н.), доставките на цифрови услуги и научните изследвания.

В момента на **европейско равнище** разглеждат още два **законодателни акта в областта на киберсигурността**. Законодателният акт за солидарност в киберпространството има за цел да укрепи капацитета за откриване, готовност и реагиране при заплахи и атаки в областта на киберсигурността. Този акт предвижда създаването на мрежа от оперативни центрове за сигурност (Европейски щит за киберсигурност) и Механизъм за спешни случаи в киберпространството, които ще подпомагат предоставянето на помощ от една държава членка на друга в случай на киберинцидент. Законодателният акт на ЕС за киберустойчивост има за цел да въведе нови правила за разработването на продукти или софтуер с цифров компонент, за да се намалят уязвимостите в областта на киберсигурността. Тази рамка включва изисквания за киберсигурност при планирането, проектирането, разработването и поддръжката на регулирани продукти и задължение за надлежна проверка през целия жизнен цикъл на такива продукти.

Националната рамка за киберсигурност в България включва **три компонента**:

- мрежова и информационна сигурност;
- киберзащита; и
- борба с киберпрестъпността.

Министерството на електронното управление е водещият **държавен орган в** областта на мрежовата и информационната сигурност. В него се помещава и Националният център за действие при инциденти в информационната сигурност (CERT България), който отговаря за дейности в четири области, а именно: предупреждение за извънредни ситуации, управление на уязвимости, управление на инциденти със сигурността и управление на данните и доказателствата за инциденти в киберпространството. ДАНС подкрепя усилията за осигуряване на киберзащита, особено по отношение на оценката на заплахите, идентифицирането, откриването и управлението на хибридни атаки в киберпространството. Такива атаки могат да приемат различни форми и да преследват различни цели, вариращи от саботаж до кражба на данни и трайно увреждане на системата. Центърът за управление и киберотбрана към Министерството

[7] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в целия Съюз, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива NIS 2), 2022 г.

на отбраната има за цел изграждане на капацитет, като осигурява обучение и програми за развитие на човешките ресурси с цел противодействие на кибератаките и засилване на превенцията. Дирекция „Киберпрестъпност“ на ГДБОП към Министерството на вътрешните работи координира предотвратяването и разследването на незаконни дейности в киберпространството, включително хакерски атаки, онлайн финансови престъпления и измами, както и нарушения на авторските права.

На **местно равнище** Лабораторията за киберсигурност в София Тех Парк е водещ доставчик на аналитични и приложни услуги за повишаване на институционалната киберсигурност и насърчаване на развитието на човешките ресурси за бизнеса и публичния сектор.

Устойчивост на критичната инфраструктура и веригите за доставки

Преди войната срещу Украйна проруски групировки извършиха кибератаки срещу украинската електропреносна мрежа, в резултат на което няколкостотин хиляди местни граждани бяха лишени от жизненоважни услуги. След нахлуването в Украйна руските сили **систематично осъществяват атаки срещу местната критична инфраструктура**. Продължаващата окупация на Запорожската атомна електроцентрала, взривяването на язовир Нова Каховка и честите нападения срещу болници, системите за съхранение и доставка на вода, електроенергия и храни, както и транспортната инфраструктура, са показателни за мащаба на военните действия. Действията на Русия също така представляват сериозна опасност за **морската безопасност и сигурност в Черно и Азовско море** и ограничават възможностите на Украйна да използва черноморските търговски пътища. Пример за това е прекратяването на сделката за износа на зърно, след като през лятото на 2023 г. Русия обяви, че спира участието си в споразумението.

Регламентите на ЕС изискват от държавите членки да **извършват оценка на риска**, която отчита опасността от хибридни или други вражески заплахи, за да определят критични субекти в секторите, които предоставят основни услуги за функционирането на обществата.[8] Ръководството на всеки субект, който е определен като критичен, следва да бъде уведомено и да извършва редовна оценка на риска поне веднъж на четири години, ако не се изисква друго съгласно националните разпоредби. Критичните субекти трябва да разполагат с вътрешни протоколи и процедури за управление на физическите и кибер рискове, и за възстановяване в случай на инцидент. Такива мерки включват и проверки на миналото на лицата, които изпълняват или кандидатстват за чувствителни позиции в критичните субекти или имат достъп до помещенията, информацията или системите за контрол на тези субекти.

В приетата през 2023 г. Стратегия за **икономическа сигурност** на ЕС се посочват четири групи взаимосвързани рискове, които изискват спешни действия, за да се гарантира устойчивостта на критичната инфраструктура и веригите за доставки, да се намали рискът от икономическа принуда

[8] Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. относно устойчивостта на критичните обекти и за отмяна на Директива 2008/114/ЕО на Съвета, 2022 г.

и да се предотврати изтичането на технологии за сигурност. Стратегията включва широк пакет от мерки, които имат за цел да укрепят механизмите за проверка на преките чуждестранни инвестиции; да противодействат на чуждестранната злонамерена намеса в научните изследвания и иновациите; и да повишат ефективността на контрола върху износа на изделия с двойна употреба и контрола върху стратегическата търговия, за да се предотврати злоупотребата с технологичния напредък за цели, които застрашават сигурността и стабилността на ЕС. ЕС също така увеличи усилията си за защита на Съюза и неговите държави членки от **икономическа принуда от страна на трети държави**.[9] ЕС създаде правна рамка за възпиране и противодействие на злоупотребата с икономически отношения, като търговия или инвестиции, с цел да се повлияе на позицията или действията на Съюза или на държава членка.

Съгласно съществуващите в България правила правителството отговаря за идентифицирането и определянето на субекти като **национална критична инфраструктура**. Компетентните органи, т.е. министерствата или други органи на изпълнителната власт, отговарят за идентифицирането на критичната инфраструктура в съответния сектор. В рамките на тази процедура всеки орган трябва да създаде постоянна работна група, която да разработи критерии и предварителен списък на потенциалните критични обекти. Министърът на вътрешните работи дава насоки относно методологията за оценка на риска, а работните групи в рамките на съответните компетентни органи разработват и предоставят методологията на собствениците/операторите на критични инфраструктури. Защитата на критичната инфраструктура е основна цел на системата за национална сигурност и няколко органа, в т. ч. ДАНС, имат водеща роля да защитават критичната инфраструктура и активите на страната.

Собствениците/операторите на критични инфраструктури са физическите или юридическите лица, които отговарят за инвестирането във или за осигуряването на нормалното функциониране, устойчивостта и целостта на система или част от система, определена като критична инфраструктура. Проверката на инвестициите в критичната инфраструктура се възлага на компетентния орган, упълномощен да администрира съответния сектор (например системите за производство и пренос на електроенергия попадат в сектора на енергетиката и се администрират от Министерството на енергетиката). През 2024 г. се очаква българският парламент да приеме законопроект за въвеждане на **национален** механизъм за **проверка (скрининг) на инвестициите**.[10]

Междуведомствената комисия за експортен контрол и неразпространение на оръжията за масово унищожение към министъра на икономиката и индустрията контролира износа, вноса, трансфера, транзита и брокерските услуги за **продукти, свързани с отбраната, и изделия и технологии с двойна употреба**. Националната агенция „Митници“ изпъл-

[9] Регламент (ЕС) 2023/2675 на Европейския парламент и на Съвета от 22 ноември 2023 г. относно защитата на Съюза и неговите държави членки от икономическа принуда от страна на трети държави, 2023 г.

[10] Център за изследване на демокрацията, Скрининг на инвестициите за повишаване на икономическата сигурност, Policy Brief No 142, декември 2023 г.

нява контролни функции за предотвратяване на незаконния трафик на стратегически стоки, включително изделия и технологии с двойна употреба.

Отбрана и управление на извънредни ситуации и кризи

Подновеният интерес на Русия към използването на ОМУ представлява значителен риск за сигурността на ЕС. Спектърът на хибридните заплахи, свързани с ОМУ, е широк. През последните години руските служби за сигурност извършиха поредица **покушения** с токсични химически, биологични и радиоактивни агенти. Това включва употребата на нервнопаралитичното вещество „Новичок“, в резултат на което са отровени няколко души и е причинена смърт и значителни материални щети.

Руските управляващи, държавните медии и прокремълските медии активно провеждат дезинформационни кампании, в които обвиняват съседните държави, включително Грузия и Украйна, в разработване на биологични оръжия, в опит да **подкопаят международното сътрудничество** в областта на здравеопазването и превенцията на болестите. От самото начало на инвазията срещу Украйна руските ядрени сили бяха поставени в повишена бойна готовност и Кремъл многократно се възползва от позицията си на ядрена държава, включително като взе решение за разполагане на ядрени оръжия в Беларус.

Неотдавна няколко репортажа посочиха, че руските войски използват сълзотворен газ срещу украинската армия. Сълзотворният газ принадлежи към групата на веществата за борба с безредиците (RCA) и международното право забранява употребата на този вид вещества като средство за водене на война.

Политиката на НАТО в областта на химическата, биологическата, радиологичната и ядрената сигурност (ХБРЯ) е всеобхватна и предоставя рамка за укрепване на **ХБРЯ отбранителни способности и устойчивостта** на държавите – членки на НАТО срещу целия спектър от ХБРЯ заплахи, в т.ч. и защита от ОМУ.[11] Политиката призовава за по-голямо и по-ефективно гражданско-военно взаимодействие и подчертава необхдоимостта от научно-техническо сътрудничество и ролята на стратегическата комуникация и публичната дипломация.

Съветът за сигурност към Министерския съвет е ключов механизъм за вземане на решения, който разработва и предлага конкретни стъпки и мерки за управлението на рискове и кризи и намаляването на заплахите за сигурността; улеснява координацията между различните компетентни органи и подпомага комуникацията при кризи. Той има водеща роля в управлението на кризи, а секретариатът му изпълнява функциите на Национален ситуационен център.

Министерството на отбраната е водещият национален орган за защита от ОМУ и ХБРЯ заплахи. Българската армия разполага с **автоматизирана информационна система за наблюдение и ранно предупрежде-**

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

ние в случай на ХБРЯ заплахи. Тази система е свързана с Националния оперативно комуникационно-информационен център на Главна дирекция „Пожарна безопасност и защита на населението“ на Министерството на вътрешните работи и улеснява обмена на данни с аналогичните системи на държавите – членки на НАТО. Военномедицинската академия към Министерството на отбраната е неразделен елемент от националната инфраструктура за управление на последствията от военни конфликти, природни бедствия, промишлени аварии и терористични атаки. Академията също така осигурява продължаващо професионално обучение в ключови области като предоставянето на здравни грижи в случай на излагане на радиация и токсични отравяния. Държавната агенция „Национална сигурност“ (ДАНС) изпълнява функциите на **Национален координационен център за противодействие на разпространението на оръжия за масово унищожение,** който отговаря за междуведомственото и многостранното сътрудничество в областта на националната сигурност и противодействието на заплахите от ОМУ.

Центърът на НАТО за управление на кризи и реагиране при бедствия (CMDR COE), който се намира в България, предлага курсове за продължаващо професионално развитие за повишаване на оперативния капацитет за готовност за управлението на извънредни ситуации и реагирането на нововъзникващи заплахи за сигурността.

Правоприлагащият сектор, включително Министерството на вътрешните работи и Националната следствена служба, както и прокуратурата, играят водеща роля в разследването на престъпни деяния, свързани със злоупотребата на химически, биологични или радиоактивни материали.

СТРАТЕГИЧЕСКИ ЦЕЛИ И СЛЕДВАЩИ СТЪПКИ

Моделът на национален подход за противодействие на хибридните заплахи, който се съсредоточава върху проактивното възпиране, трябва да включва поне **три стратегически цели**: (1) превенция, (2) разкриване и (3) предотвратяване (Фигура 2). Изпълнението на тези цели изисква координирани усилия в четирите области на действие и активното участие на правителството и заинтересованите страни от гражданското общество в преодоляването на риска от злонамерена намеса. От съществено значение е да се въведат подходящи политики и мерки за смекчаването на отрицателните въздействия на хибридната война и улесняването на бързото възстановяване в случай на инцидент. Изграждането на многопластова национална система, която има за цел да ограничи риска от злонамерена намеса, е ключов възпиращ фактор срещу заплахата от хибридна война.

Фигура 2: Елементи на интегрирания подход за противодействие на хибридните заплахи

Източник: Център за изследване на демокрацията.

Постигането на всяка от трите стратегически цели изисква **набор от съответни основни способности** и активизиращи фактори, които улесняват процеса на поддържане на основните способности:

- За **превенцията** на хибридни заплахи, България трябва да осигури следните **основни способности**:

- o събиране на разузнавателна информация и наблюдение на средата на сигурност за бързо идентифициране на заплахите, свързани с чуждестранна злонамерена намеса;
- o междуведомствена координация и обмен на данни между компетентните органи и заинтересованите страни за подобряването на разбирането за хибридните заплахи и начина, по който те могат да се проявят;
- o планиране на отбраната, при което се отчита спектърът на хибридните заплахи и се стимулира придобиването на подходящ оперативен и технически капацитет;
- o стратегически комуникации, които отчитат риска от чуждестранни операции за манипулиране на информация и кампании за дезинформация;
- o осведоменост за заплахите и медийна грамотност на обществено равнище, които повишават чувствителността към чуждестранна злонамерена намеса, включително дезинформация.

Основните **фактори**, които допринасят за устойчивостта на тези способности, включват: (1) внедряване на системи за разузнаване, наблюдение и разузнаване чрез стратегически ангажименти с партньори от ЕС и НАТО; (2) политически и регулаторни мерки, които осигуряват прозрачност на чуждестранните инвестиции, обществените поръчки и финансирането на политическите партии; (3) прилагане на правната и процедурната рамка за борба с корупцията, прането на пари и заобикалянето на санкции във всички сектори; (4) стандартизиране и лицензиране на дейностите, свързани с експлоатацията и поддръжката на критични обекти; (5) регулаторни и институционални мерки по отношение на собствеността и финансирането на медиите.

- За **разкриването** на хибридни заплахи, България трябва да разполага със следните **основни способности**:
  - o общонационална система за ранно предупреждение;
  - o периодичен преглед на изпълнението на политиките, регламентите и протоколите за справяне с хибридните заплахи, за да се гарантира, че съответните мерки и инициативи са актуални;
  - o електронна система за документиране на минали атаки в областта на хибридната война за подпомагане на разследването на подозрителни дейности.

Основните **фактори**, които допринасят за устойчивостта на тези способности, включват: (1) институционални и секторни механизми за докладване на подозрителни дейности, свързани с чуждестранна злонамерена намеса; (2) интегриран национален механизъм за междусекторна оценка на уязвимостта; (3) стимули за заинтересованите страни да насърчават практики и поведение за подобряване на сигурността, с цел противодействие на чуждестранната злонамерена намеса.

- За **предотвратяването** на хибридните заплахи, България трябва да осигури следните **основни способности**:
  - ресурсно обезпечени междуведомствени екипи и звена за бързо реагиране в случай на хибридна атака;
  - кризисна комуникация в случай на хибридна война;
  - механизми за осъществяване на международна помощ и сътрудничество в случай на хибридна война.

Основните **фактори**, които допринасят за устойчивостта на тези способности, включват: (1) стратегия за управление на кризи, която се фокусира върху пресичането на опити за чуждестранна намеса; (2) разследвне и разкриване на дейности, свързани с чуждестранна намеса, и наказателно преследване на отговорните за тези дейности лица; (3) междусекторни инициативи за противодействие на дезинформацията в медиите и киберпространството.