РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

УНИВЕРЗИТЕТ “СВ.КИРИЛ И МЕТОДИЈ – СКОПЈЕ “

ФИЛОЗОФСКИ ФАКУЛТЕТ-СКОПЈЕ

ИНСТИТУТ ЗА БЕЗБЕДНОСТ ОДБРАНА И МИР

СТУДИСКА ПРОГРАМА БЕЗБЕДНОСЕН МЕНАЏМЕНТ

МАГИСТЕРСКА РАБОТА

Тема: Градење капацитети за справување и отпорност од хибридни закани

Студент: Лидија Милева

Досие број: 5586/24

Проф. д-р Оливер Бакрески

Скопје, април 2026 година

С О Д Р Ж И Н А

ВОВЕД

Магистерската работа има за цел да ја анализира состојбата за справување со хибридните закани на национално ниво, како и на ниво на НАТО и ЕУ. Во текот на изработката собрав и анализирав документи од релевантни институции во Република Северна Македонија, НАТО и ЕУ, истражувачки центри и организации што работат на прашања поврзани со хибридните закани и дезинформации, како што се Центарот за извонредност на НАТО за стратегиски комуникации (NATO StratCom Center of Excellence), Центарот за извонредност за борба против хибридни закани (Hybrid CoE), независната новинска агенција Мета.мк, организацијата за човекови права и слободи ЦИВИЛ – Центар за слобода и др. Овие документи се движат од официјални извештаи и соопштенија за медиумите до говори и интервјуа за медиумите дадени од претставници на ЕУ и НАТО, како и од домашните институции.

Темата за хибридни закани, доминира во безбедносниот пејзаж во Европа во последниве години. Не е изненадување што денешните хибридни закани припаѓаат на сферата на сериозни и акутни закани за ЕУ, НАТО и нивните земји-членки и се препознаени како такви од креаторите на политики низ цела Европа и пошироко.

Денес, стратешката конкуренција, сеприсутната нестабилност и повторливите шокови ја дефинираат поширокаата безбедносна средина. Заканите можат да доаѓаат од државни и недржавни актери во форма на терористички напади, сајбер напади или хибридна војна, што може да ги замагли границите помеѓу конвенционалните и неконвенционалните форми на конфликт. Климатските промени и природните катастрофи како што се поплавите, пожарите и земјотресите ја нагласуваат важноста на цивилно-воениот ангажман и соработка. Отпорноста на општествата, во сложената комплексна безбедносна средина, продолжува да биде сериозно тестирана, вклучително и од пандемии. Нашите општества станаа уште поповрзани и меѓузависни со широката примена на новите технологии во економскиот, финансискиот, информатичкиот и сајбер доменот, но покрај придобивките, тоа создадва ранливости и може да воспостави зависности.

Неодамнешните настани го пренасочија вниманието кон предизвиците поблиску до територијата на НАТО. Алијансата го зајакнува својот став за одвраќање и одбрана, вклучително и преку зајакнување на цивилната подготвеност и националната отпорност.

Отпорноста се потпира на силна соработка меѓу цивилните и воените засегнати страни, што е од заемна корист, како во мирно време, така и во време на криза. Како што покажа пандемијата COVID-19, воената помош за цивилните власти може да биде од критична поддршка кога цивилните ресурси се под сериозен притисок. Во исто време, цивилната поддршка е од суштинско значење за овозможување и одржување на воените

сили на НАТО во време на криза, без разлика дали преку цивилна експертиза или пристап до критични комерцијални услуги и инфраструктура.

Сојузниците на НАТО ги преиспитуваат сопствените ранливости и подготвеност за ефикасно одвраќање и одбрана од современите безбедносни закани. Тие ги засилуваат своите напори за борба против хибридните закани преку ажурирање на стратегиите, зајакнување на нивната одбрана и инфраструктура, донесување ново законодавство и прилагодување на структурите за координација и донесување одлуки.

Растечките хибридни закани вклучуваат: сајбер напади, саботажи, електронско мешање во глобалните навигациски и сателитски системи, дезинформациски кампањи и политичка и индустриска шпионажа, како и миграцијата како оружје.

Земјите-членки на НАТО реагираат национално, мултилатерално и колективно за да се справат со ризикот од хибридна војна во нејзините различни форми. Градењето капацитети за справување и отпорност од хибридни закани е првенствено национална одговорност, со импликации врз регионалната и колективната отпорност.

Во денешната безбедносна средина, ефикасна и одржлива отпорност, побарува целосен опсег на воени и цивилни способности, како и пристап на целото општество, кој вклучува активна соработка низ владата, приватниот сектор и цивилното општество.

Дополнителни, ЕУ, НАТО и другите мултилатерални организации имаат на располагање бројни средства за справување со хибридните закани, така што колективното дејствување во политички, дипломатски или економски домени, мултинационалното припишување или стратешкото испраќање пораки честопати може да биде поефикасно од националниот напор.

ГЛАВА I

Општо за хибридни закани

Денес, Европа се соочува со растечки и сè посложени безбедносни предизвици. Хибридните закани станаа составен дел од нашите безбедносни грижи; војната се врати во Европа; нестабилноста се зголемува во соседните региони на Европа; има обиди за манипулирање со резултатите од изборите; а демократиите сè повеќе се прикажуваат како слаби системи за управување. Можноста за ширење на дезинформации брзо и со голем дострел преку социјалните медиуми дополнително го влошува потенцијалното влијание на хибридните закани. Покрај тоа, нашата зголемена зависност од IT алатки за нашата секојдневна работа, банкарство, управување со здравството, како и за изборите и управувањето, значи дека секоја европска, земја-членка и компанија е изложена на одреден ризик да биде погодена од хибридни закани. Исто така, треба да бидеме свесни дека влијанието на хибридните закани не се само ограничени на безбедносниот домен, туку е поврзано и со одбраната.[1]

Хибридното војување е сеопфатен термин што вклучува операции во конфликт кои не се однесуваат на традиционалните разбирања на војната. Познато и како операции во сива зона, конфликт со низок интензитет или воени операции освен војна (MOOTW), хибридното војување вклучува неограничена употреба на различни, но меѓусебно поврзани методи кои честопати ги замаглуваат конвенционалните домени во конфликтот (Hoffman 2006 и 2007; Mattis and Hoffman 2005). Хибридното војување вклучува принудни методи кои комбинираат регуларни и нерегуларни сили, воени и невоени тактики и насилни и ненасилни субверзивни и криминални дејствија под стратешка насока за постигнување политички или воени цели во современото бојно поле.[2]

Новите алатки, концепти и технологии насочени кон ранливостите го зголемуваат досегот и ефикасноста на денешните хибридни закани во постигнувањето на стратешки и сеопфатни цели како што се поткопување на јавната доверба во демократските институции, продлабочување на нездравата поларизација и на национално и на меѓународно ниво, предизвикување на основните вредности на демократските општества, стекнување геополитичко влијание и моќ преку повредување

[1]Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G., Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023 стр.6, https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf, посетена на 19/2/2023

[2] Dolan C. J., Hybrid warfare in the Western Balkans: How structural vulnerability attracts maligned powers and hostile influence, SEEU Review, 2022, стр.5

и поткопување на другите и влијание врз способноста за донесување одлуки на политичките лидери.

Сојузниците на НАТО се соочуваат со закани и предизвици и од државни и од недржавни актери кои користат хибридни активности за да ги таргетираат политичките институции, да влијаат на јавното мислење и да ја поткопаат безбедноста на граѓаните на НАТО. Хибридните методи на војување - како што се пропаганда, измама, саботажа и други невоени тактики - долго време се користат за дестабилизација на противниците, но она што е ново во нападите во последниве години е нивната брзина, обем и интензитет, олеснети од брзите технолошки промени и глобалната меѓусебна поврзаност.

Во согласност со дефиницијата на Европскиот центар за извонредност за справување со хибридни закани, хибридните закани се штетни активности што се планираат и спроведуваат со малигна намера. Тие имаат за цел да ја поткопаат целта, како што е држава или институција, преку различни средства, честопати комбинирани. Таквите средства вклучуваат манипулација со информации, сајбер напади, економско влијание или принуда, тајни политички маневри, принудна дипломатија или закани со воена сила. Хибридните закани опишуваат широк спектар на штетни активности со различни цели, почнувајќи од операции на влијание и мешање, па сè до хибридно војување.[3]

1. Поим за хибридни закани и отпорност

Терминот хибридна закана се однесува на акција спроведена од државни или недржавни актери, чија цел е да ја поткопа или да ѝ наштети на целта преку влијание врз нејзиното донесување одлуки на локално, регионално, државно или институционално ниво. Таквите активности се координирани и синхронизирани и намерно се насочени кон ранливоста на демократските држави и институции. Активностите може да се одвиваат, на пример, во политички, економски, воени, цивилни или информативни домени. Тие се спроведуваат со користење на широк опсег на средства и се дизајнирани да останат под прагот на откривање и припишување. Хибридното дејство се карактеризира со двосмисленост, бидејќи хибридните актери ги замаглуваат вообичаените граници на меѓународната политика и дејствуваат во интерфејс меѓу надворешното и внатрешното, легалното и нелегално и мирот и војната. Нејасноти јата се создава со комбинирање на конвенционални и неконвенционални средства, дезинформации и мешање во политичка дебата или избори, критични нарушувања или

[3] MAFART J., Hybrid threats: from geopolitics to internal security, Schuman Paper бр.819, 2026, стр.6 https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-819-en.pdf

напади на инфраструктурата, сајбер-операции, различни форми на криминални активности и, конечно, асиметрична употреба на воени средства и војување.[4]

Хибридните закани влегоа во лексиконот на НАТО во 2010 година, првично дефинирајќи ги како „оние што ги претставуваат противниците, со можност истовремено да користат конвенционални и неконвенционални средства адаптивно во остварувањето на нивните цели“. Ова беше во контекст на „меѓусебната поврзаност на глобализираната средина“, олеснета од брзите технолошки промени што овозможија зголемување на брзината, обемот и интензитетот на нападите.[5]

Највлијателната референтна точка за НАТО и нациите е почетокот на тековните акции на Русија во Украина во 2014 година, што стана архетипски пример за хибридно „војување“. Концептот на хибридно „војување“ во овој контекст се прошири надвор од фокусирањето на употребата на претежно воени инструменти за да вклучи политички, економски и социјални системи.[6]

Првиот документ на ЕУ за хибридните закани објавен како документ “food-for-thought” од страна на Европската служба за надворешно дејствување (EEAS) во 2015 година беше резултат на голем број земји-членки на ЕУ (вклучувајќи ги Финска и балтичките земји-членки) кои ја повикуваа ЕУ да формулира заеднички одговор против хибридните закани, особено во однос на отпорноста на земјите-членки и стратешките комуникации на ЕУ. Во документот експлицитно се наведува дека „безбедносната средина во Европа драматично се промени“, споменувајќи прво инвазијата и анексијата на Крим, а потоа подемот на групата Исламска држава и придружниот феномен на европски странски борци како клучни случувања што бараа заеднички одговор. Овој акцент на единството на ниво на ЕУ ја повтори претходната изјава на високата претставничка на ЕУ за надворешни работи, Федерика Могерини, дека „во сегашната безбедносна средина и соочена со нови и сложени закани, единството е потребно повеќе од кога било“. Сите земји имаат ранливости. Тие во голема мера варираат и се движат од економски и енергетски зависности, голема зависност од критична инфраструктура во клучни области, како што се финансиите, енергијата, комуникациите или транспортот, до многу суптилните и чувствителни прашања во рамките на земјите, поврзани со интеграцијата на религиозните или етничките групи или недостатоците во почитувањето на човековите права. [7]

[4] Митревска М. и Милевски Т.,Кон отпорност и заштита на критичната инфраструктура, 2022, стр.43-44
[5] Heap B., Hansen P., Gill M., Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, NATO StratCom COE, 2010, стр.12 https://stratcomcoe.org/cuploads/pfiles/Strategic-Communications-Hybrid-Threats-Toolkit_Rev_12l.pdf
[6] Исто.,стр.12
[7] (EEAS(2015) 731), https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf, посетена на 19/2/2026

Во 2016 година, Европската комисија ја објави својата рамка за справување со хибридни закани, опишувајќи ја „мешавината од принудна и субверзивна активност, конвенционални и неконвенционални методи (т.е. дипломатски, воени, економски, технолошки), кои можат да се користат на координиран начин од страна на државни или недржавни актери за да се постигнат специфични цели, а воедно да останат под прагот на формално прогласена војна. Обично се става акцент на искористување на ранливостите на целта и на генерирање двосмисленост за да се попречат процесите на донесување одлуки. [8]

Во коминикето на НАТО од Брисел во 2018 година беше истакнато дека „Нашите нации се соочуваат со зголемен предизвик од државни и недржавни актери кои користат хибридни активности кои имаат за цел да создадат двосмисленост и да ги замаглат границите меѓу мирот, кризата и конфликтот“. Ова беше повторно потврдено на состанокот на лидерите во Лондон во 2019 година од Генералниот секретар Столтенберг, велејќи дека НАТО треба да го засили својот одговор на хибридните закани. [9]

Во 2020 година, Европскиот центар за борба против хибридните закани објави модел за да го опише пејзажот на хибридните закани, опишувајќи ги како стари колку и конфликтите и војувањата, препакувани и зајакнати со променлива динамика на безбедносната средина, нови алатки, концепти и технологии, таргетирање на ранливостите со цел поткопување на јавната доверба во демократските институции, продлабочување на нездравата поларизација предизвикување на основните вредности на демократските општества, стекнување геополитичко влијание и моќ преку повредување и поткопување на другите и влијание врз способноста за донесување одлуки на политичките лидери.[10]

Хибридните закани по природа се од надворешно потекло и се третираат како такви во релевантните одбранбени форуми. Во Стратешкиот концепт, НАТО јасно наведува – како одговор на двосмисленоста на користените методи – дека „хибридните операции против сојузниците би можеле да достигнат ниво на вооружен напад и би можеле да го наведат Северноатлантскиот Совет да се повика на Член 5 од Северноатлантскиот Договор“. Неодамнешните упади со беспилотни летала во воздушниот простор на некои европски држави се впечатлив пример за вакви операции и одговорот што тие можат да го предизвикаат во воената сфера; но сега можеме да заклучиме од доктрината на НАТО дека колективниот одговор од страна на неговите

[8] European Commission (2016), Joint Communication to the European Parliament and the Council, joint framework on countering hybrid threats. стр.1.
[9] NATO Press. (2019, December 4). Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Heads of State and/or Government. NATO https://www.nato.int/en/news-and-events/events/transcripts/2019/12/04/press-conference
[10] European Union and Hybrid COE (2020) The Landscape of Hybrid Threats: A Conceptual Model. p.4.

членови не е незамислив - барем во принцип и над одреден праг на сериозност - во случај на комбинација од хибридни дејствија кои би можеле да бидат поподмолни, како што се саботажи, сајбер напади или мешање во изборна кампања од големи размери. Хибридните закани беа признати и во Стратешкиот компас на Европската Унија.[11]

Основните карактеристики на хибридните закани се: координирана и синхронизирана акција која намерно ја таргетира системската ранливост на демократските држави и институции преку широк опсег на средства; активности кои ги искористуваат праговите на откривање и припишување, како и различните интерфејси (војна-мир, внатрешна-надворешна безбедност, локално-државно и национално-меѓународно); активности насочени кон влијание на различни форми на одлучување на локално (регионално), државно или институционално ниво, дизајнирани да продолжат и/ или да ги исполнат стратешките цели на актерот додека ја поткопуваат и/или повредуваат целта.[12]

2. Видови на хибридни закани

Хибридните закани комбинираат воени и невоени, како и тајни и отворени средства, вклучувајќи дезинформации, сајбер напади, економски притисок, распоредување на нерегуларни вооружени групи и употреба на редовни сили. Хибридните методи се користат за замаглување на границите помеѓу војната и мирот и се обидуваат да посеат сомнеж во умовите на целните популации. Тие имаат за цел да ги дестабилизираат и поткопаат општествата. Брзината, обемот и интензитетот на хибридните закани се зголемија во последниве години. Подготвеноста за спречување, спротивставување и одговор на хибридни напади, без разлика дали од државни или недржавни актери, е врвен приоритет за НАТО.[13]

На пример, Руската Федерација користи софистицирани хибридни стратегии, вклучувајќи политичко мешање, злонамерни сајбер активности, економски притисок и принуда, субверзија, агресија и анексија. Принудната воена позиција и реторика се користат и како дел од хибридните стратегии на Руската Федерација за остварување на своите политички цели и поткопување на меѓународниот поредок базиран на правила. Хибридни и сајбер операции на Народна Република Кина (НР Кина) и нејзината конфронтациска реторика и дезинформации се насочени кон сојузниците и штетат на безбедноста на Алијансата. На пример, НР Кина се стреми да контролира клучни технолошки и индустриски сектори, критична инфраструктура и стратешки материјали

[11] MAFART J., Hybrid threats: from geopolitics to internal security,2026, стр.2 https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-819-en.pdf, посетена на 21/2/2026
[12] https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ посетена на 20/2/2026
[13] https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats, посетена на 21/2/2026

и синџири на снабдување. Таа ја користи својата економска моќ за да создаде стратешки зависности и да го зголеми своето влијание.[14]

Хибридните закани се насочени кон ранливости и системски слабости во една нација. Противниците се свесни за овие ранливости и може да ги испитаат и да ги искористат подоцна. Институционалната слабост во примената на принципите на стратешките комуникации може да биде ранливост, како и довербата на јавноста во владеачката власт.

Согласно Анализата на студиите на случаи изнесени во Комплетот алатки за стратешки комуникации за хибридни закани, Примена на принципите на стратешките комуникации на НАТО за разбирање и справување со заканите од сивата зона идентификувани се следниве клучни видови хибридни закани:[15]

Вид на хибридна закана	**Стратешка логика**
Директно влијание на јавното мислење	- Воспоставување, финансирање или поддршка на академски, образовни или културни институции. - Дезинформации; лажни вести или кампањи со дезинформации. - Воспоставување или поддршка на медиуми и новински канали; сопственишство на медиуми и рекламни кампањи; притисок врз новинари.
Влошување на општествените поделби	- Финансирање, поддршка или промовирање на национални, религиозни или политички екстремистички организации. - Поларизација на политичките дебати за поткопување на одредена политичка програма. - Експлоатација на етнички или културни идентитети за поткопување на социјалната кохезија.
Агитација и граѓански немири	- Агитација на целна општествена, културна, религиозна или етничка група за повикување на промена на политиката или за иницирање протести во целната нација. - Нарушување на политичките или економските процеси преку протести или бојкоти. - Ризик од радикализација или ескалација на насилство.
Мешање во избори	- Странско мешање во изборите за да се влијае врз гласачкото однесување на населението.
Намалување на довербата на јавноста во владата	- Намалување на довербата на јавноста во владата и војската; дискредитација на целната влада и јавните институции. - Поткопување на кредибилитетот и легитимитетот на политиките и операциите.

[14] Исто.,
[15] Heap B., Hansen P., Gill M., Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, стр.10-11

	- Создавање јавна несигурност; скандали со поткуп и корупција; уцена и изнуда. and extortion.
Поткопување на управувањето и државните функции	- Спонзорство од страна на странска држава на политичка партија или актер. - Корупција и криминални мрежи, организиран криминал. - Воспоставување на паралелни неформални владини структури преку информациски, образовни и здравствени системи.
Дипломатски притисок	- Намалување на дипломатскиот и домашниот опсег на дејствување на целната влада преку притисок, закана со употреба на сила, заплашување или принуда; влошување на зависностите. - Дискредитирање на владата за оштетување на меѓународниот углед, влошување на односите со меѓународните партнери и сојузници. - Ризик да стане платформа за конфликт преку посредник; регионална нестабилност.
Економска моќ	- Економски притисок; економска или енергетска зависност; употреба на санкции или стимулации; нарушување на деловните операции. - Екстракција на вредни ресурси од спорни територии. - Маргинализација на локалната работна сила; создавање неформални услови за работа за локалните работници во изворната земја, создавајќи здравствени и безбедносни ризици. - Влошување или создавање економски нееднаквости и слаба економија (нерамномерен регионален развој, социјална нееднаквост, сиромаштија).
Сајбер операции	- Прекин на комуникациските текови и друга дигитална инфраструктура. - Сајбер напади како изјава за намера и способност. - Психолошки ефект врз граѓаните и инвеститорите; јавна несигурност и намалување на довербата, политичка непријатност.
Тероризам и насилен екстремизам	- Национален, религиозен и политички екстремизам. - Ризик од домашен тероризам; повторно оживување на поранешни терористички организации. - Етнички мотивирани акти на насилство; ескалација на социо-политички протести; секташко насилство.
Шпионажа	- Финансиски, физички, безбедносни и репутациски загуби поврзани со шпионски активности; намалување на јавната доверба. - Корпоративна, сајбер и политичка шпионажа.
Територијални спорови	- Регионална нестабилност; прелевање на ефекти врз други територијални спорови; сепаратистички региони во рамките на државните граници. - Зајакнати сепаратистички движења.

Извор: Heap B., Hansen P., Gill M., Strategic Communications Hybrid Threats Toolkit, Applying the principles of NATO Strategic Communications to understand and counter grey zone threats, стр.10-11

Хибридните закани се манифестираат во различни форми и можат да се појават различно во зависност од нивниот контекст. Овие закани варираат не само според разновидниот спектар на тактики, туку и според актерите што ги извршуваат овие закани. Хибридното и конвенционалното војување може да се спроведуваат исклучиво од државни актери или преку соработка на државни и недржавни субјекти, вклучувајќи терористички групи, паравоени организации и криминални мрежи. Овие актери ја искористуваат отвореноста и меѓусебната поврзаност на демократските општества, користејќи напредни технологии и глобални комуникациски мрежи за да го зголемат своето влијание. Ефикасноста на хибридните закани лежи во нивната способност да работат под прагот на традиционалните воени одговори, со што се избегнува директна конфронтација и откривање. Ова ја нагласува потребата од сеопфатен и интегриран пристап кон отпорноста и одбраната, осигурувајќи дека општествата се опремени да се справат и ублажат повеќеслојната природа на хибридните закани.[16]

На Западен Балкан, Хибридното војување претставува збир на нискобуџетни акции или тактики дизајнирани да ја поткопаат јавната доверба во институциите, да ги ослабнат нормите и да го попречат интегрирањето со НАТО и ЕУ. Тактиките на хибридна војна вклучуваат употреба на дезинформации, сајбер напади, операции на влијание и наративи за жртва за да се поткопаат евроатлантските институции, да се развијат предрасуди за конфликт, да се промовира раздор и да се одржат замрзнати конфликти. Хибридното војување им овозможува особено на Русија и во помала мера на Кина и на Турција, да ги остварат своите политики, да ги искористат поделбите, да ја ослабнат отпорноста или да се промовираат себеси и своите претпочитани наративи.[17]

3. Справување со хибридните закани

За ефикасна борба против хибридните закани, од суштинско значење е да се препознае дека овој процес вклучува три критични фази: препознавање (признавање), мапирање и справување. Секоја од овие фази е составен дел од градењето робусна и адаптивна рамка за отпорност способна да се спротивстави на сложената и динамична природа на хибридните закани. Со методично напредување низ овие фази, креаторите на политики и засегнатите страни можат подобро да ги заштитат демократските

[16] Khidasheli T., HYBRID THREATS AND RESILIENCE, Safeguarding Democratic Values in a Connected World, Friedrich-Naumann-Foundation for Freedom South Caucasus 2024, стр.6
[17] Dolan C. J., Hybrid warfare in the Western Balkans: How structural vulnerability attracts maligned powers and hostile influence, SEEU Review, 2022, стр.6

вредности и да го одржат интегритетот на нивните општества во услови на еволуирачки предизвици.[18]

Првиот и основен чекор во градењето успешна отпорност е признавање на комплексноста и се поприсутната природа на овие закани. Оваа фаза вклучува длабоко и систематско разбирање на средината во која дејствуваат хибридните закани. Потребно е идентификување на ранливостите во рамките на политичкото, економското и социјалното ткиво и технолошките системи на општеството што противниците би можеле да ги искористат. Препознавањето не е само за свест, туку и за разбирање на меѓузависностите и потенцијалните каскадни ефекти што хибридните закани можат да ги имаат низ различни сектори. Со препознавање на целиот опсег на овие закани, креаторите на политиките и засегнатите страни можат подобро да ги предвидат начините на кои хибридните тактики би можеле да се манифестираат и да ги нарушат демократските процеси.[19]

Откако ќе се препознаат сложеноста и потенцијалните ранливости, следната клучна фаза е мапирањето. Ова вклучува детална анализа и документација на специфичните патишта преку кои хибридните закани би можеле да навлезат и да влијаат врз општеството. Мапирањето вклучува идентификување на клучните актери, државни и недржавни, кои можат да бидат вклучени во распоредувањето на хибридни тактики и разбирање на нивните мотивации, способности и стратегии. Исто така, бара темелна проценка на ресурсите и методите на овие актери, како што се сајбер алатки, кампањи за дезинформации, економски притисок или сили на посредници. Ефективното мапирање обезбедува стратешки преглед што помага во визуелизирање како различните елементи на хибридните закани се меѓусебно поврзани и каде тие би можеле да се спојат за да создадат значајни влијанија. Оваа фаза е клучна за развивање на насочени и проактивни мерки за ублажување на ризиците. [20]

Последната фаза во борбата против хибридните закани е справување со идентификуваните предизвици преку координиран и сеопфатен пристап. Оваа фаза вклучува спроведување практични мерки за зајакнување на отпорноста и спротивставување на специфичните ранливости и закани што се препознаени и мапирани. Справувањето со хибридните закани бара повеќеслојна стратегија што може да вклучува подобрување на сајбер безбедноста, подобрување на интегритетот на информациите, градење на јавната свест и поттикнување на меѓународната соработка. Исто така, вклучува развивање и спроведување на законски и регулаторни рамки што се прилагодуваат на еволутивната природа на хибридните закани. Покрај тоа,

[18] Khidasheli T., HYBRID THREATS AND RESILIENCE, Safeguarding Democratic Values in a Connected World, Friedrich-Naumann-Foundation for Freedom South Caucasus 2024, стр.12
[19] Исто.,
[20] Исто.,

справувањето со овие закани бара пристап на целото општество, вклучувајќи не само владини агенции, туку и субјекти од приватниот сектор, организации од граѓанското општество и поширокаta јавност.[21]

Ефикасното справување со хибридните закани подразбира како прво детекција на заканата, потоа способност за одбивање на заканата, насочен кон градење отпорност и на крајот одговор на заканата. [22]

Детекција на заканата

Клучен момент при справувањето со хибридни закани е детекцијата. Како начин за справување со хибридните закани, детекцијата подразбира поседување способност за добивање релевантни и навремени информации за потенцијалните намери на напаѓачот од сите области и носители.

Методот кој треба да се користи за успешно детектирање хибридни закани вклучува идентификување на критичните национални ранливости, поврзување на ранливостите со можни сценарија и претпоставки за целите и способностите на напаѓачот и определување индикатори за поврзување на ранливостите и мерките кои треба да се преземат за справување со хибридните закани. Создавањето и развивањето способност за детекција е приоритетна активност, бидејќи без детекција на заканата не е можно да се планира одговор за ефикасно спротивставување на истата.

Одбивање на заканата

Способноста за одбивање на заканата е метод насочен кон градењето отпорност, создавање капацитети да се поднесе стрес и способност за надминување на нанесените штети од заканите, како и способност за возвраќање на напаѓачот. Отпорноста е потребна, пред сè, во областите кои се таргетирани за хибриден напад, како: политиката, економијата, одбранбено-безбедносниот сектор, информативниот сектор, граѓанското општество и критичната инфраструктура. Способноста за неутрализирање на нападите подразбира поседување капацитети за менаџирање со ефектите од: напад со неконвенционални воени сили, терористички напади, напади на изборниот процес, напади врз финансискиот сектор, сајбер-напади, напади со ХБРН-оружје, информативни операциии, предизвикување насилен екстремизам и радикализација, како и поделби во општеството. Со поседување на овие способности ќе се намали негативниот ефект од евентуалните хибридни напади. Клучниот фактор за одбивање на хибридните закани е поседувањето способност да се казни напаѓачот. Тоа значи креирање инструменти за нанесување штета на субјектот кој користи хибридни методи, со цел неговите

[21] Исто., стр.12
[22] Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.22-23

активности да бидат неисплатливи, бидејќи штетата би ја надминала добивката. Поседувањето таква способност би го одвратило потенцијалниот напаѓач од користење хибридни активности против државата, бидејќи истите би биле неефективни.

Сведоци сме дека секојдневните манифестации на природните и човечките опасности може да резултираат со значителна штета и нарушување на заедниците, вклучително и нивните згради, инфраструктурните системи, на економијата и достапноста на социјалните услуги.

Тргнувајќи од овие констатации, концептот на отпорност на заедницата, кој вклучува планирање за отпор, апсорбирање и брзо закрепнување од нарушувачките настани, се стекна со актуелност во последната деценија низ целиот свет.

Одговор на заканата

Одговорот на хибридните закани значи постоење на ефективен процес за донесување одлуки на стратешко ниво. Клучен фактор во овој процес е поседување кредибилна процена за состојбата и одредување ниво на толеранција на заканата, чие надминување би означувало дека земјата е предмет на напад со користење хибридни методи. Поседувањето кредибилни и навремени информации за хибридни закани против државата ќе го помогне процесот на одлучување, како и процесот при активирање на механизмите за помош од ЕУ и колективниот систем за одбрана на НАТО. Како одговор на хибриден напад може да се користат различни механизми, како економски санкции кон држави, компании и лица, протерување дипломати, информативни операции и други активности за неутрализирање на хибридните закани. Меѓутоа, суштински важно е одговорот да се моделира на начин кој нема да предизвика ескалација на заканата, туку ќе го примора напаѓачот да ги прекине хибридните активности поради нивна неефективност, бидејќи штетата која ќе ја трпи поради таквите активности ќе биде поголема од потенцијалната добивка.

Слика бр.1. Извор: Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.24

Дополнително, предвидувањето бара соработка на сите нивоа, низ повеќе министерства и низ различни линии на напори, следејќи сеопфатен пристап низ дипломатскиот/политичкиот, информативниот, воениот, економскиот, финансискиот, разузнавачкиот и правниот спектар. Националните, билатералните и колективните напори на Алијансата мора да бидат интегрирани и меѓусебно да се зајакнуваат.

4. Градење на капацитети за справување со хибридните закани

НАТО и Европската Унија го идентификуваа справувањето со хибридните закани како приоритет за соработка од 2016 година.

Иницијативата за воспоставување на Центар за извонредност за справување со хибридни закани произлезе од Заедничката комуникација на Европската комисија и високиот претставник со- Европскиот парламент и Советот „Заедничка рамка за справување со хибридни закани - одговор на Европската Унија“ (Брисел, 6 април 2016 година).[23]

[23] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Joint Framework on countering hybrid threats a European Union response, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018, посетена на 21/2/2026

Иницијативата беше поддржана во Заедничкиот сет предлози за спроведување на Заедничката декларација на ЕУ/НАТО, одобрена од Советот на Европската Унија и Северноатлантскиот совет на 6 декември 2016 година.[24]

Во согласност со заедничката комуникација, Центарот за извонредност за справување со хибридни закани, би се фокусирал на развој на отпорност и градење капацитети за справување со хибридни закани преку истражување и практична обука и вежби со учесници од повеќе сектори. Центарот, исто така, би го зајакнал усогласувањето помеѓу приватниот и јавниот, цивилниот и воениот, како и академскиот сектор.

Центарот за извонредност за справување со хибридни закани (Hybrid CoE) се воспостави на 2 октомври 2017 година. Од 2017 година, бројот на земјите учеснички постојано се зголемува. Естонија, Норвешка и Шпанија се приклучија на Центарот во јули 2017 година; Холандија, Италија, Данска, Чешка, Австрија, Канада, Романија и Кипар во текот на 2018 година; Грција, Унгарија, Луксембург, Црна Гора, Португалија, Словенија и Турција во текот на 2019 година, Словачка во 2020 година; Хрватска, Белгија, Исланд во 2021 година; Малта во 2022 година; Ирска во 2023 година; Бугарија во 2023 година; Северна Македонија во 2023 година; и Албанија во 2024 година. Во февруари 2026 година, САД се повлекоа од Центарот за извонредност за справување со хибридни закани. Дополнително, на Украина ѝ е доделен статус на засилено партнерство по руската инвазија во 2022 година.[25]

Клучната задача на Центарот е да ги изгради способностите на земјите-учеснички за спречување и спротивставување на хибридните закани. Ова се постигнува со споделување на најдобрите практики, давање препораки, како и тестирање на нови идеи и пристапи. Центарот, исто така, ги гради оперативните капацитети на земјите-учеснички преку обука на практичари и организирање практични вежби. Центарот не само што создава нови стратешки концепти, туку помага и за нивно спроведување. Извонредноста се постигнува преку меѓувладините, меѓусекторските мрежи на Центарот, кои се состојат од над 3.000 практичари и експерти кои работат во земјите-учеснички, ЕУ и НАТО, приватниот сектор и академијата. Центарот за извонредност за хибридни закани го предводи разговорот за хибридните закани преку објавување на широк опсег на публикации и ангажирање со различни партнери на терен. [26]

[24] JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION, https://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf, посетена на 21/2/2026
[25] https://www.hybridcoe.fi/establishment/, посетена на 21/2/2026
[26] https://www.hybridcoe.fi/who-what-and-how/посетена на 21/2/2026

Работата на Центарот е планирана и координирана од Секретаријатот на Hybrid CoE, лоциран во Хелсинки, Финска. Центарот моментално има три мрежи на Заедници на интерес (COI): Хибридно влијание; Ранливости и отпорност; и Стратегија и одбрана. Заедниците на интерес се состојат од мрежи на практичари од земјите-учеснички, како и од ЕУ и НАТО. Тие обезбедуваат простор за мултинационално и мултидисциплинарно споделување на најдобрите практики, искуство и експертиза, така што земјите-учеснички и организациите можат подобро да ги разберат и да се спротивстават на хибридните закани. Тие исто така обезбедуваат простор за координирање на акциите.[27]

Во насока на подобрување на способноста на Европа да спречува и да реагира на новите закани на 26 март 2025 година беше објавена Стратегијата на Унијата за подготвеност,[28] која има Акционен план и за да се постигне визијата презентирана во Стратегијата на Унијата за подготвеност, Комисијата, Високиот претставник и земјите-членки треба да ги спроведат активностите наведени во Анексот, вклучувајќи индикативна временска рамка за имплементација. Стратегијата се фокусира на интегриран пристап кон сите опасности, пристап на целата влада, кој ги обединува сите релевантни актери, на сите нивоа на власт (локално, регионално, национално и ЕУ) и пристап на целото општество, кој ги обединува граѓаните, локалните заедници и граѓанското општество, бизнисите и социјалните партнери, како и научните и академските заедници.

Високата претставничка за надворешни работи и безбедносна политика/потпретседател на Европската комисија, Каја Калас, во однос на Стратегијата на Унијата за подготвеност на ЕУ за спречување и реагирање на нови закани и кризи истакна „Денес се соочуваме со сè поголем број надворешни безбедносни предизвици и сè поголем број хибридни напади во нашиот заеднички европски простор. Јасно е дека Европа мора да биде посилна на сите фронтови и на секое ниво на општеството. Секогаш е подобро да се спречат кризите отколку да се справуваме со нивните последици. Стратегијата на ЕУ е за градење сеопфатна слика за заканите со кои се соочуваме, подготовка на граѓаните, вклучително и преку подобрување на нивната свест за ризик, зајакнување на цивилно-воената соработка и потесна соработка со надворешни партнери, вклучително и НАТО. Подготвеноста е предизвик за целата влада и целото општество - денес ние се залагаме за колективен одговор“[29] .

Клучни цели и активности на Стратегијата се следните:

[27] https://www.hybridcoe.fi/our-work/posetena na 21/2/2026
[28] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the European Preparedness Union Strategy, 26.3.2025
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0130, посетена на 21/2/2026
[29] https://www.eeas.europa.eu/eeas/preparedness-union-strategy_en, посетена на 21/2/2026

Заштита на основните општествени функции на Европа:

- Развивање на минимални критериуми за подготвеност за основни услуги како што се болници, училишта, транспорт и телекомуникации;

- Зголемување на складирањето на критична опрема и материјали;

- Подобрување на климатската адаптација и достапноста на критични природни ресурси како што е водата.

Промовирање на подготвеноста на населението:

- Охрабрување на јавноста да усвои практични мерки, како што е одржување на основните залихи најмалку 72 часа во итни случаи;

- Интегрирање на часовите за подготвеност во училишните наставни програми и воведување на Ден на подготвеност на ЕУ.

Подобрување на координацијата за одговор на кризи:

- Воспоставување на кризен центар на ЕУ за подобрување на интеграцијата меѓу постојните кризни структури на ЕУ.

Зајакнување на цивилно-воената соработка:

- Спроведување редовни вежби за подготвеност на ниво на ЕУ, обединувајќи ги вооружените сили, цивилната заштита, полицијата, безбедноста, здравствените работници и пожарникарите;

- Олеснување на инвестициите со двојна намена;

- Зајакнување на можностите за предвидување;

- Развивање на сеопфатна проценка на ризикот и заканите на ниво на ЕУ, помагајќи во спречувањето на кризи како што се природни катастрофи или хибридни закани.

Зголемување на јавно-приватната соработка:

- Создавање на јавно-приватна работна група за подготвеност;

- Формулирање на протоколи за итни случаи со бизнисите за да се обезбеди брза достапност на основните материјали, стоки и услуги и обезбедување на критични производствени линии.

Зајакнување на соработката со надворешни партнери:

Работа со стратешки партнери како НАТО за воена мобилност, клима и безбедност, нови технологии, сајбер, вселена и одбранбена индустрија.[30]

Принципите утврдени во „Заедничката рамка“ од 2016 година остануваат целосно релевантни: „Доколку борбата против хибридните закани се однесува на националната безбедност и одбрана и одржувањето на законот и редот, примарната одговорност лежи кај земјите-членки, бидејќи повеќето национални ранливости се специфични за секоја земја. Сепак, многу земји-членки на ЕУ се соочуваат со заеднички закани, кои можат да бидат насочени и кон прекугранични мрежи или инфраструктури. Ваквите закани можат да се решат поефикасно со координиран одговор на ниво на ЕУ преку користење на политиките и инструментите на ЕУ.“[31]

Како што е наведено во „Комуникацијата за Стратегијата на ЕУ за безбедност“[32] и „Стратешки компас за безбедност и одбрана“[33], гледаме брз развој на настаните и зголемено ниво на софистицираност кај хибридните закани, затоа отпорноста кон хибридните закани треба да се дизајнира и имплементира на сите нивоа и мора да ги земе предвид мерките за отпорност, не само од перспектива на повеќе домени, туку и како сеопфатен пристап на екосистемот. Развивањето отпорност кон хибридните закани бара гледање подалеку од отпорноста во поединечните области, градејќи ја системски, додека се земаат предвид зависностите и меѓузависностите меѓу различните делови од општеството.

За да помогнат во спротивставувањето на хибридните закани и поддршката на креаторите на политиките во одбраната на демократските општества, Европскиот центар за извонредност за справување со хибридни закани (Hybrid CoE) и Заедничкиот истражувачки центар на Европската комисија изградија модел кој препорачува рамка за сеопфатно преиспитување на отпорноста. Сеопфатен екосистем за отпорност, или Comprehensive Resilience Ecosystem (CORE), истакнува два фактори кога размислуваме за одговор: Прво, отворените општества се секогаш повеќе поврзани внатрешно и меѓусебно и второ секој одговор треба да го вклучи целото општество за ефикасно спротивставување на заканите. За таа цел, претставениот модел се однесува на различни

[30] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_856, посетена на 21/2/2026
[31] MAFART J., Hybrid threats: from geopolitics to internal security, Schuman Paper n°819, 2026, стр.6, https://server.www.robert-schuman.eu/storage/en/doc/questions-d-europe/qe-819-en.pdf, посетена на 22/2/2026
[32] COMMUNICATION FROM THE COMMISSION on the EU Security Union Strategy, COM(2020) 605, достапна на https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605
[33] A STRATEGIC COMPASS FOR SECURITY AND DEFENCE, достапна на https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

општествени или секторски „простори“ (институции, граѓанско општество, услуги), како и различни „нивоа“ (меѓународно, национално и локално).[34]

Перспективата на екосистемот е план за адаптивно размислување и разбирање на начините на кои земјите-членки на ЕУ можат индивидуално и колективно да ја поттикнат отпорноста и да ја зголемат својата маргина на маневрирање во борбата против хибридните закани. Моделот CORE може да послужи како стратешка контролна табла за одлучување кои ресурси, алатки и мерки да се мобилизираат во услови на активности на хибридни закани. Понатаму, може да ја обезбеди потребната концептуална основа за градење на сеопфатен пристап кон отпорноста што го опфаќа целото општество. На ниво на ЕУ, оваа перспектива би можела да го истакне опсегот на потенцијални решенија, мерки и алатки што би можеле да се мобилизираат за борба против хибридните закани.[35]

Генерално, и Стратешкиот компас на ЕУ и Стратешки концепт на НАТО[36] ја зголемуваат способноста на двете организации да се справат со широкиот спектар на закани и предизвици со кои се соочуваат во моментов. Со оглед на тоа што ЕУ и НАТО делат многу од овие закани и предизвици, некои преклопувања се неизбежни во документите, што покажува дека и ЕУ и НАТО се фокусирани на наоѓање решенија за заедничките предизвици, но играат различни улоги во безбедноста и одбраната на Европа и имаат различни надлежности. Хибридните и сајбер заканите се нешто што и Стратешкиот компас на ЕУ и Стратешкиот концепт на НАТО го адресираат.

Во изминатиот период, имаше интензивирање на хибридните активности на Русија - од сајбер напади и кампањи за манипулација со информации и мешање до случаи на палење, саботажа, вклучително и на критична инфраструктура, како и инструментализација на миграцијата и други деструктивни активности. ЕУ продолжи да го користи својот хибриден пакет алатки за подобрување на колективната ситуациска свест околу хибридните закани и развој на координиран одговор на активностите на Русија. За да ги поддржи своите партнери кои се соочуваат со слични закани, ЕУ, исто така, за прв пат распореди свои хибридни тимови за брз одговор за да се справат со специфичните непосредни потреби и да ја подобрат подготвеноста и отпорноста на Молдавија против хибридни закани.[37]

[34] Попоска В., ИНФОРМИРАНА ОДБРАНА, Вовед за хибридните закани за критичната инфраструктура, Информативна студија, Што се хибридни закани, а што критична инфраструктура и како изгледа новата безбедносна архитектура?, Скопје 2024, стр.11
[35] Hybrid threats: a comprehensive resilience ecosystem, March 2023 https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf, посетена на 21/2/2026,стр.89
[36] NATO 2022 Strategic Concept, достапен на: https://www.act.nato.int/wpcontent/uploads/2023/05/290622-strategic-concept.pdf
[37] HR(2025) 148, https://www.parlament.gv.at/dokument/XXVIII/EU/28161/imfname_11496795.pdf, стр. 39, посетена на 11/3/2026

На највисоко ниво, директорите, меѓу кои се комесарите на ЕУ, генералниот секретар на ЕЕАС и авторитетите на НАТО, како што е заменик-генералниот секретар на НАТО, се состануваат најмалку двапати годишно, обезбедувајќи стратешко водство и управување со односите ЕУ-НАТО и надгледувајќи го спроведувањето на 74-те акции и предлози вклучени во заедничките декларации на двете страни.

Сегашниот 10-ти извештај за спроведувањето на 74-те заеднички предлози - кои беа одобрени од Советите на ЕУ и НАТО во паралелни процеси во 2016 и 2017 година – елаборира за значителниот напредок постигнат помеѓу јуни 2024 и мај 2025 година преку демонстрирање на конкретни резултати низ целиот спектар на агендата за соработка. Ангажманот на персоналот на ЕУ и НАТО дополнително се прошири, меѓу другото, преку започнување на нови структурирани дијалози, кои сега опфаќаат отпорност; воена мобилност; климатски промени, безбедност и одбрана; нови и револуционерни технологии; вселена; сајбер; и одбранбена индустрија, како и преку редовна координација помеѓу двете организации за Украина.[38]

5. Заштита и отпорност од хибридни закани преку националната, цивилна подготвеност

Отпорноста е една клучна компонента за справување со хибридните закани. Отпорноста кон хибридните закани може да ги искористи мерките за отпорност на различни домени. Развивањето на отпорноста кон хибридните закани бара не само да се разгледа отпорноста во секоја област, туку и како таа да се изгради системски, земајќи ги предвид зависностите и меѓузависностите помеѓу различните делови од општеството.[39]

Националната, цивилната подготвеност е долгогодишна област на работа за владите на НАТО. Алијансата ја операционализираше својата работа за отпорност преку цивилната подготвеност од 2014 година, особено преку седумте основни барања што ги одразуваат националните функции од витално значење за националната и колективната одбрана.[40]

Во 2016 година, членките на НАТО се согласија за упатствата за отпорност и се обврзаа да ги исполнат основните барања за национална отпорност.[41] Тие дополнително

[38] https://www.consilium.europa.eu/media/f54kvokr/250605-progress-report-nr10-eu-nato.pdf, стр.1, посетена на 21/3/2026
[39] Hybrid threats: a comprehensive resilience ecosystem, March 2023, https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf, посетена на 21/2/2026
[40] Hunter Christie E, Berzina K, NATO and Societal Resilience: All Hands on Deck in an Age of War, https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf, посетена на 21/2/2026
[41] NATO, Warsaw Summit Communiqué, July 9, 2016, paragraph 73, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique, посетена на 21/2/2026

се согласија за зајакната обврска за отпорност во 2021 година. Постојат седум основни барања за национална отпорност според кои треба да се мери нивното ниво на подготвеност, кои ги одразуваат основните функции на континуитет на владата, основните услуги за населението и цивилната поддршка на војската.[42]

Овие основни барања ги одразуваат трите основни функции на цивилната подготвеност што мора да се одржуваат дури и во најтешките услови: континуитет на владата, основни услуги за населението и цивилна поддршка на војската. Овие три основни функции и седумте основни барања (7BLR) се поврзани. Ова значи дека ако една област е погодена, друга може да биде погодена како резултат на тоа. На пример, влијанието врз снабдувањето со енергија може да влијае на способноста за справување со масовни жртви и други деструктивни здравствени кризи.[43]

Седумте основни барања (7BLR):[44]

Седумте основни барања за национална отпорност претставува столб на пристапот на НАТО кон отпорност преку цивилната подготвеност и обезбедува индикатори за земјите-членки на НАТО врз основа на кои тие можат да ја измерат својата моментална состојба на отпорност и да ги идентификуваат можните празнини и области за подобрување.

1 – Обезбеден континуитет на владата и критичните владини служби

Основната цел е да се обезбеди способност за донесување одлуки, нивно соопштување и нивно спроведување во криза. Овој услов комбинира неколку клучни цели.

1) Формализиран план за продолжување на владините операции, вклучувајќи го наследувањето на политичкото раководство, делегирањето на овластувањата и приоритизацијата на клучните владини институции за одржување на основните функции (војска, храна, вода, транспорт, инфраструктура, медицина, индустрија итн.).

2) Ефективна и доверлива јавна комуникација во кризни ситуации. Националните мерки за управување со кризни ситуации бараат поддршка од населението за да бидат ефикасни. Комуникацијата во кризни ситуации е клучна за да се постигне ова јавно прифаќање, но за да се постигне тоа, „довербата“ на луѓето е клучна.

[42] NATO, Resilience and civil preparedness – Article 3, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3, посетена на 21/2/2026
[43] Исто.,
[44] CIMIC Handbook, CIMIC Centre of Excellence (CCOE) стр.86-89
https://www.cimic-coe.org/wp-content/uploads/2025/03/cimic-handbook.pdf, посетена на 21/2/2026

3) Образован и обучен цивилен и воен персонал, способен да управува со критична инфраструктура и да ја обнови кога е оштетена од непријателски напади. Трајното онеспособување на критичните инфраструктури може да доведе до јавна деморализација и губење на поддршката за владата. На крајот на краиштата, ова ќе ја попречи ефикасната одбрана.

4) Робустен и самостоен центар за управување со кризни ситуации за да се обезбеди капацитет за цивилна команда и контрола. Објектот треба да биде заштитен од низа закани (кинетички напади, ХБРН или сајбер напади).

Тоа поразбира обезбеден континуитет на владата и критичните владини услуги: на пример, способност за донесување одлуки и комуникација со граѓаните во криза.

2 – Отпорно снабдување со енергија

Енергијата е фундаментален овозможувач на воената способност и затоа е критичен фактор во воените операции. Способноста на НАТО да ја заштити и одржи потребната енергија за своите операции зависи од гарантираната испорака на енергија без оглед на растојанието, теренот или непријателските дејствија.

За да се минимизираат негативните ефекти од кризата со снабдувањето со енергија, мора да се исполнат пет цели:

1) Безбеден пристап до сигурни извори на енергија. Распределувањето на ризиците преку диверзификација на рутите, добавувачите и ресурсите ја зголемува сигурноста во време на криза;

2) Постоењето на робусни и одржливи системи за редундантност помага да се минимизира штетата во случај на дефект. Ова вклучува планови за управување со кризи и обучен персонал за нивно управување;

3) Познавањето на критичните точки во синџирите на снабдување, зависностите од (можни странски) добавувачи на енергија и меѓузависностите помеѓу енергетскиот сектор и другите сектори се од суштинско значење за ефикасно планирање и приоритизирање на кризните мерки;

4) Брзиот пристап до безбедни информации е клучен за добивање заеднички преглед на кризата во развој и мерките преземени од сите вклучени засегнати страни. Треба да се воспостават процеси за споделување информации, да се управува со овластувањата, протоколите да бидат јасни за сите вклучени, а информациските системи треба да бидат достапни врз основа на потребата за знаење;

5) Идентификација на ризиците и можностите што новите технологии можат да ги имаат врз отпорните енергетски системи. Постарите системи можат да бидат нарушени од новите технологии, но развојот на нови технолошки решенија може навистина да се забрза и за време на подолготрајни кризни ситуации (на пр. автономно работење на микро мрежи).

Отпорни снабдувања со енергија подразбира обезбедување континуирано снабдување со енергија и резервни планови за управување со прекини.

3 – Способност за ефикасно справување со неконтролирано движење на луѓе

Управувањето со масовното движење е важно за војската. Воените сили можат да бидат вклучени во помагањето на бегалците и управувањето со нивното безбедно преминување до области каде што можат да добијат помош и заштита. Ефективното управување со масовното движење на луѓето може да помогне во спречувањето на ширењето на болести, ублажување на страдањето и намалување на ризикот од насилство или конфликт. Одржувањето на стабилноста во погодените региони, исто така, придонесува за безбедноста и слободата на движење на воениот персонал и цивилите.

Две цели се централни:

1) Постоење на национален план што им овозможува на одговорните цивилни власти да обезбедат способност за предвидување, следење, деконфликт и ефикасно справување со ненадејно и/или продолжено неконтролирано движење на луѓе, од и надвор од националната територија. Ова вклучува масовен прилив на луѓе што надминува 2% од националното население, преку цивилни и воени аранжмани за непредвидени ситуации, капацитети и капацитет за зголемување. Овој план треба да содржи обезбедување храна, вода, засолниште, транспорт, медицински установи, безбедност итн.

2) Цивилно-воена координација и планирање што овозможува безбеден транзит на бегалци по релевантни транспортни правци, без попречување на воените сили или нивно изложување на воено насилство.

Масовното движење на луѓето може да биде под влијание на голем број фактори:

1) мотивацијата за масовното движење (на пр. природни опасности, конфликт, економски нееднаквости, политичка нестабилност, недостаток на безбедност);

2) ситуациите со кои се соочуваат луѓето додека се во движење (на пр. достапност на безбедни правци, храна и вода, ризик од експлоатација, ширење на екстремизам);

3) вклучување на надворешни актери (на пр. политиките на соседните земји или поддршката од меѓународни организации).

Ова значи способност за ефикасно справување со неконтролирано движење на луѓе и деконфликтирање на овие движења од воените распоредувања на НАТО.

4 – Отпорни ресурси за храна и вода

За да се обезбеди снабдување со вода и храна, треба да се исполнат три цели:

1) систем за идентификување и пријавување на контаминација на вода и храна;

2) план за обезбедување дека снабдувањето со храна и вода е достапно од алтернативни извори;

3) сеопфатен план за непредвидени ситуации кој го зема предвид губењето на дел од потребната работна сила, експертскиот капацитет и потребните ресурси за производство на вода и храна за одржување на снабдувањето. Секторските меѓузависности со снабдувањето со енергија и транспортот, како и контролата на централните функции на системот за снабдување од страна на странски сопственици, исто така, треба да бидат вклучени во планирањето.

Отпорни ресурси за храна и вода значи: обезбедување отпорни снабдувања кои се безбедни од прекини или саботажи;

5 – Отпорност за справување со масовни жртви

За да бидат подготвени за инциденти со масовни жртви, земјите-членки на НАТО треба да ги почитуваат петте основни цели:

1) Градење отпорност преку цивилна подготвеност за ефикасно справување со масовни жртви, т.е. доволен персонал и хируршки капацитет, достапност на транспорт, земање предвид на религиозните аспекти на погребите итн.;

2) Треба да биде оперативен системот за рано предупредување и известување за да се алармира населението, националните даватели на услуги на терен, операторите на критична инфраструктура и војската;

3) Треба да се создаде база на податоци за следење на цивилните медицински капацитети (број на болнички кревети, персонал, медицинска опрема, единици за изолација, лаборатории, капацитети за транспорт и евакуација итн.). Доколку се достапни, може да се додадат воени капацитети. Оваа база на податоци треба често да се ажурира и да

содржи информации во реално време, веродостојни за капацитетите на здравствената заштита во текот на целата криза;

4) Мора да постојат цивилно-воени планови за да се овозможи континуирано функционирање на сите медицински релевантни услуги;

5) Секоја држава треба да има робусни национални линии за снабдување со медицински материјали. Во овој контекст, постојните ранливости во синџирот на снабдување треба да бидат вклучени во анализата за да се обезбеди најдобра можна подготвеност.

Покрај физичките аспекти, други фактори можат да имаат директно влијание врз воената операција. Може да има емоционални и ментални последици, на пример, ако луѓето не можат да ги погребаат своите изгубени најблиски или не сакаат да ја потврдат нивната смрт. Овие секундарни ефекти можат да го одложат процесот на закрепнување и да ја поткопаат отпорноста на заедницата за враќање во состојба на нормалност.

Во проценката на CIMIC не треба да се решат само масовните жртви, туку и ефектите врз населението и врз општествената отпорност. Влијанието врз воената операција треба да се земе предвид при советување на командантот.

Отпорност за справување со масовни жртви и деструктивни здравствени кризи значи: обезбедување дека цивилните здравствени системи можат да се справат и дека доволно медицински материјали се складирани и безбедни;

6 – Отпорни цивилни комуникациски системи

Централна компонента во поддршката на отпорноста е пристапот до комуникациите и нивното одржување:

1) Пристапот до безбедна, сигурна комуникациска инфраструктура е од најголема важност и во време на мир, криза и конфликт под сите можни закани. Пристапот до комуникациската инфраструктура треба да биде приоритетен за да се обезбеди способност за команда и контрола;

2) Комуникациската инфраструктура треба да биде заштитена од упади, прекини, деградација или пречки за да се обезбедат доволни услуги за функциите на HN (Host Nation) и НАТО C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance);

3) Неопходно е да може брзо да се реагира на дефекти во телекомуникациската технологија. Посебно внимание ќе се посвети на ризиците што ги претставуваат новите

технологии, особено кога сите критични компоненти на системот сè под странска или приватна контрола;

Отпорни цивилни комуникациски системи подразбира: обезбедување дека телекомуникациите и сајбер мрежите можат да функционираат дури и во кризни услови, со доволен резервен капацитет. Ова исто така вклучува потреба од сигурни комуникациски системи, вклучувајќи 5G, робусни опции за враќање на овие системи, приоритетен пристап до националните власти во време на криза и темелни проценки на сите ризици за комуникациските системи;

7 – Отпорни системи за цивилен транспорт

Инфраструктурите и системите за цивилен транспорт се клучни и за цивилната употреба и за способноста на војската да маневрира низ областа на операции:

1) Националната регулатива треба да постави приоритети во областа на транспортот во случај на криза или конфликт. Ова треба да обезбеди силите на НАТО да можат брзо и ефикасно да ги преминат границите на земјите-членки на Алијансата и да транзитираат низ нејзината територија. Исто така, обезбедува потребни движења за реализација на други основни барања (на пр. снабдување со храна и вода);

2) Националните регулативи бараат законска примена;

3) Воената употреба на инфраструктурата и системите за цивилен транспорт бара планирање. Планерите на CIMIC треба да се координираат со другите мали и средни претпријатија (на пр. MOVE, ENGR, MED), земајќи ги предвид општите оперативни фактори (расположив персонал, стратешки капацитет за подигнување, мултимодални транспортни врски итн.) и фактори специфични за видот на користениот транспорт;

4) Потребно е цивилно-воено планирање за да се воспостави поддршка од земјата домаќин (HNS) и да се обезбеди воена употреба на системи за цивилен транспорт. Новите технологии како што се вештачката интелигенција (ВИ), автономните системи на оружје, големите податоци, биотехнологиите и квантните технологии го менуваат светот и начинот на кој функционираат НАТО и неговите земји-членки.

Отпорни системи за цивилен транспорт значи: обезбедување дека силите на НАТО можат брзо да се движат низ територијата на Алијансата и дека цивилните служби можат да се потпрат на транспортните мрежи, дури и во криза.[45]

[45] CIMIC Handbook, CIMIC Centre of Excellence (CCOE) стр.86-89
https://www.cimic-coe.org/wp-content/uploads/2025/03/cimic-handbook.pdf, посетена на 21/2/2026

НАТО основните барања имаат две карактеристики: тие се од суштинско значење за општеството кое е под напад да продолжи да функционира и да ја ублажи штетата врз цивилите, и се директно релевантни за континуитетот на воените операции.[46]

Поструктуриран пристап беше одобрен од сојузниците на самитот на НАТО во Мадрид на крајот на јуни 2022 година. Според овој нов пристап, сојузниците ќе бидат повикани да дефинираат национални цели за отпорност и планови за имплементација и да ги споделат овие цели и планови со персоналот на НАТО и едни со други преку новоформираниот Комитет за отпорност на алијансата. Персоналот на НАТО ќе изготвува стратешка проценка на отпорност на ниво на алијансата на секои четири години која ќе им обезбеди на воените власти на НАТО појасна слика за отпорноста на алијансата. [47]

[46] Christie E.H., Berzina K, NATO and Societal Resilience: All Hands on Deck in an Age of War, Policy Brief, GMF, 2022, стр.4 , https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf, посетена на 21/2/2026

[47] Исто.,

ГЛАВА II

Заштита на критичната инфраструктура од хибридни закани

1. Општо за критичната инфраструктура

Терминот „критична инфраструктура“ е релативно нов и теоретичаритеги наоѓаат неговите корени во средината на деведесеттите години и е тесно поврзан со енергетската безбедност, телекомуникациите, енергетските системи, гасоводите и нафтоводите, економијата, транспортот, водоводот и сл. Токму од тие причини „критичната инфраструктура“ и нејзината ефикасност се од големо значење за квалитетот на животот, стопанството и функционирањето на јавниот сектор. Секако дека денешниот турбулентен свет и динамичен развој, со сè поголема пенетрација на модерните технологии и вештачката интелигенција, со зголемен број на неспецифични закани и ризици, како и сè поголемиот ефект од климатските промени кој резултира со зачестени катастрофи и со зголемен интензитет и огромни штети и загуби, влијаат поимот „критична инфраструктура“ да е сè поприсутен во секојдневниот живот.[48]

2. Сектори на критична инфраструктура

Европската Унија ја дефинира критичната инфраструктура преку Директивата за определување и идентификување на европската критична инфраструктура од 2008 година [49], која ги повикува државите членки да ја идентификуваат и определат критична инфраструктури, која ја имаат на сопствената територија, како и да извршат проценка на потребата за подобрување на нејзината заштита. Сите држави членки ја спроведоа Директивата преку воспоставување процес за идентификување и назначување на европска критична инфраструктура во енергетскиот и транспортниот сектор. Во самата Директива, критичната инфраструктура е дефинирана како: „средство, систем или дел од него лоциран во државите членки што е од суштинско значење за одржување на виталните општествени функции, здравјето, безбедноста, економската или социјалната благосостојба на луѓето и чие нарушувањето или уништување би имало значително влијание во државата членка како резултат на неуспехот да се одржат тие функции“. Директивата посебно ја препознава европската критична инфраструктура (ЕКИ) како критична инфраструктура чие нарушување или уништување би имало прекугранично

[48] Митревска М., Милевски Т, Микац Р., Критична инфраструктура:Концепт и безбедносни предизвици, 2019, стр.19.

[49] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345/75, 23.12.2008, достапна на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114, посетена на 22/2/2026

ефект и која треба, како таква, да биде издвоена и идентификувана преку заедничка процедура.

Кон крајот на 2022 година, Европската комисија отиде чекор понапред дефинирајќи ги критичните ентитети како покомплексна форма на критична инфраструктура со зголемена меѓу зависност. Директивата за отпорност на критични субјекти (CER) 2022/2557[50] утврдува хармонизирани минимални правила за подобрување на отпорноста на критичните субјекти. Сајбербезбедноста се третира одделно преку новата Директива за мрежни и информациски системи (NIS2)[51] .

Директивата CER стапи во сила на 16 јануари 2023 година и бараше од земјите-членки да ги транспонираат нејзините одредби во националното законодавство до 17 октомври 2024 година. Како и со многу сложени европски директиви што вклучуваат институционално реструктуирање и меѓусекторска координација, процесот на транспонирање се покажа како нееднаков низ целата Унија. Иако рокот формално е истечен, имплементацијата останува нецелосна во неколку земји-членки, што ги одразува обемните институционални, регулаторни и оперативни прилагодувања потребни за интегрирање на Директивата во националните правни системи. Директивата воспоставува сеопфатна рамка дизајнирана да обезбеди субјектите што обезбедуваат основни услуги да можат да спречат, да издржат, да одговорат и да се опоравт од нарушувања предизвикани од природни опасности, несреќи, саботажи, тероризам и други хибридни закани. За да се постигне оваа цел, земјите-членки мора да усвојат национални стратегии за отпорност на критичните субјекти, да спроведат национални проценки на ризик што опфаќаат обезбедување основни услуги, да назначат надлежни органи одговорни за надзор и спроведување и да ги идентификуваат критичните субјекти што работат во рамките на нивната јурисдикција. Голем број земји-членки веќе усвоија законска регулатива за спроведување и ја воспоставија институционалната архитектура што ја бара Директивата. Други воведоа нацрт-законодавство што во моментов е во процес на парламентарен преглед или регулаторни консултации. Трета група земји-членки доживеа доцнења во законодавниот процес, честопати затоа што владите избрале да ја интегрираат Директивата CER во пошироки законски пакети што се однесуваат на заштитата на инфраструктурата, цивилната заштита и управувањето со сајбер безбедноста. Еден фактор што придонесува за доцнењата е блиската врска помеѓу Директивата CER и Директивата (ЕУ) 2022/2555 (Директивата NIS2) што ги утврдува

[50] 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, OJ, L 333/164, 27.12.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557, посетена на 22/2/2026

[51] 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), OJ, L 333/80, 27.12.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555, посетена на 22/2/2026

барањата за сајбер безбедност за операторите на основните и важните субјекти. Поради преклопувањето на целите, неколку земји-членки избраа да ги транспонираат обете директиви преку координирани законодавни реформи, процес што неизбежно го продолжи целокупниот временски рок за имплементација.[52]

Комисијата предложи неисцрпна листа на услуги кои се клучни за одржување на виталните општествени функции, економските активности, јавното здравје и безбедност или животната средина, за единаесетте сектори и потсектори опфатени со Директивата, како што следува: [53]

1. **Енергетски сектор**, со услуги како што се производство на електрична енергија и складирање на енергија;

2. **Транспортен сектор**, со услуги како што се управување и одржување на аеродромска или железничка инфраструктура;

3. **Банкарски сектор**, со основни услуги како што се примање депозити и позајмување;

4. **Сектор за инфраструктура на финансискиот пазар**, со услуги како што се работење на места за тргување и на клириншки системи;

5. **Здравствен сектор**, со дистрибуција, производство, обезбедување здравствена заштита и медицински услуги;

6. **Сектор за вода за пиење**, со снабдување со вода за пиење и дистрибуција на вода за пиење;

7. **Сектор за отпадни води**, со услуги за собирање, третман и отстранување на отпадни води;

8. **Сектор за дигитална инфраструктура**, со услуги како што се обезбедување и работење на услуга за интернет размена, систем на доменски имиња, домен од највисоко ниво, cloud computing и центар за податоци;

9. Услуги во **секторот за јавна администрација**;

10. **Вселенски сектор**, со работење на услуги за копнена инфраструктура;

[52] https://www.critical-entities-resilience-directive.com/, посетена на 21/3/2026
[53] https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3992, посетена на 21/3/2026

11. **Производство, преработка и дистрибуција на прехранбениот сектор**, со големо индустриско производство и преработка на храна, услуги за синџирот на снабдување со храна и услуги за дистрибуција на храна на големо.

Откако ќе бидат назначени, критичните субјекти мора да спроведат: [54]

Проценки на ризик: Субјектите мора да идентификуваат физички и оперативни закани, вклучувајќи ги и оние што потекнуваат од нивните синџири на снабдување.

Планирање на отпорност: Да документираат како ќе спречат, ќе одговорат на и ќе се опоравт од прекини.

Физичка заштита: Спроведување соодветни контроли, од надзор до планирање во итни случаи.

Евалуација на добавувачи: Проширување на призмата на ризик со вклучување на клучните трети страни и зависности.

Пријавување на инциденти: Известување на властите во рок од 24 часа од значителното прекинување на услугата и поднесување целосен извештај во рок од еден месец.

Важно е да се напомене дека CER препознава дека многу критични нарушувања ги преминуваат границите. Доколку организацијата работи во шест или повеќе земји-членки, може да бидете класифицирани како „критичен субјект од особено европско значење“, предмет на дополнителен надзор и координација на ниво на ЕУ.[55]

Заедно со регулативата DORA -Digital Operational Resilience Act (директно применлива и специфична за секторот регулатива, насочена кон банкарството, инфраструктурите на финансиските пазари и дигиталната инфраструктура)[56] и директивата NIS2, Директивата за отпорност на критични субјекти (CER) претставува уште еден клучен законодавен инструмент што бара внимателна подготовка. Секоја земја-членка, до јануари 2026 година, мора да развие стратегија за подобрување на отпорноста на критичните субјекти и последователно, до јули 2026 година, тие се

[54] Understanding the CER Directive: What It Means for Critical Infrastructure in Europe, блог, достапна на: https://humanrisks.com/blog/the-cer-directive-what-it-means-for-critical-infrastructure-and-supply-chain-resilience-in-europe/, посетена на 21/3/2026
[55] Исто,.
[56] REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L 333/1, 27.12.2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554, посетена на 22/2/2026

должни да состават список на критични субјекти. Последниот чекор е да се достави извештај за усогласеност со барањата на директивата до Европската комисија најдоцна до јули 2027 година.

Директивата CER ги наведува правно обврзувачките барања за националните власти на начин на кој пристапот на НАТО кон отпорноста не го прави тоа. Сепак, напредокот на НАТО кон националните цели за отпорност и плановите за имплементација, како и нивното споделување и прегледување колективно и со персоналот на НАТО, се совпаѓа со слични цели според директивата, особено обврската за креирање национални стратегии кои ги утврдуваат целите и мерките на политиката за подобрување на отпорноста.

НАТО треба да ги гледа случувањата на ниво на ЕУ делумно како предизвик, но главно како можност. Предизвикот е што спроведувањето на Директивата CER ќе ги привлече националните власти на членките на алијансата на ЕУ во повеќе дискусии во рамките на ЕУ, потенцијално намалувајќи го релативното влијание на консултациите на НАТО во заедничкото дефинирање на најдобрите практики за цивилните перспективи за секторите што се од интерес на ниво на ЕУ и НАТО. Со цел да се максимизира вредноста на двата процеса, персоналот на НАТО треба да развие добра свест за дискусиите на ниво на ЕУ, особено оние на Групата за отпорност на критични субјекти. Со вложување на таков напор, може да стане полесно да се дефинира додадената вредност што НАТО може да ја донесе на членките на алијансата на ЕУ, особено во цивилната подготвеност како што традиционално се третира и во поопширното поле на општествена отпорност. Важно е да се оцени обемот и ефективноста на основните барања на НАТО во однос на предвидливите потреби и степенот до кој тие доволно ги структурираат националните напори. Првото прашање е дали дополнителни функции треба да се додадат на седумте основни барања. Разлики во покриеноста се појавуваат кога се споредуваат тие со десетте сектори предложени од Европската Комисија. Отпадните води се наведени во Директивата CER, но не се посебна функција за НАТО. Отпадните води треба да се решаваат заедно со ресурсите за храна и вода: нарушувањата во нивното управување можат да влијаат на достапноста на вода за пиење за цивилни и воени потреби. Понатаму, воените инсталации имаат свои сопствени потреби за третман на отпадни води. Отпадните води се тема што треба да биде од поголем интерес на ниво на ЕУ и НАТО. Директивата CER, исто така, ги наведува банкарските и финансиските пазарни инфраструктури, кои не се опфатени со основните барања на НАТО. Вооружените сили постојано бараат, дури и во големи борбени операции, можност за

вршење и примање плаќања. Затоа, НАТО треба да разгледа ново основно барање насочено кон отпорни системи за плаќање.[57]

Во врска со спроведувањето на Директивата CER на ЕУ, секоја членка на алијансата на ЕУ треба да биде охрабрена да обрне соодветно внимание на сценаријата на вооружен напад врз нејзината територија или на вооружен напад против членка на ЕУ или сојузник на НАТО, овозможувајќи проценките на ризикот и другите резултати својствени за директивата да бидат соодветни за целта. Во врска со тоа, треба да има тесна соработка и брифинзи помеѓу Меѓународниот штаб на НАТО и претставникот на Европската комисија кој ќе претседава со Групата за отпорност на критични субјекти. Треба да се додадат три нови функции на основните барања на НАТО: системи за плаќање, психолошка одбрана и континуитет на софтверот за податоци и инфраструктура. Секоја од нив се однесува на важен аспект на општествената отпорност, а воедно е релевантна од перспектива на овозможување на одбраната. Треба да има поголема употреба на квантитативни индикатори за мерење на напредокот во исполнувањето на основните барања на НАТО за секој сојузник.[58]

Многу клучни компоненти на цивилната инфраструктура, вклучувајќи железници, пристаништа, аеродроми и енергетски мрежи, за време на Студената војна, беа во владини раце и лесно можеа да се пренесат под контрола на НАТО во кризна или воена ситуација. По распадот на Советскиот Сојуз, значително намалената конвенционална воена закана за Алијансата доведе до намалување на инвестициите во цивилна подготвеност и зголемена зависност од комерцијални актери за обезбедување критични услуги и инфраструктура:

- Околу 90 проценти од воениот транспорт за големи воени операции се обезбедува од цивилни средства изнајмени или реквизирани од комерцијалниот сектор;

- Над 70 проценти од сателитските комуникации што се користат за одбранбени цели се обезбедени од комерцијалниот сектор;

- Приближно 95 проценти од трансатлантскиот интернет сообраќај, вклучувајќи ги и воените комуникации, се пренесува преку подводни мрежи со оптички влакна, од кои повеќето се во сопственост и управувани од субјекти од приватниот сектор;

[57] Christie E.H., Berzina K, NATO and Societal Resilience: All Hands on Deck in an Age of War, Policy Brief, GMF, 2022, стр.8
[58] Исто.,стр.11

- Во просек, околу 75 проценти од поддршката на земјата домаќин за операциите на НАТО се добива од локална комерцијална инфраструктура и услуги.[59]

Продолжувајќи го овој тренд, како што заканите од меѓународниот тероризам стануваа поприсутни, сојузничките операции сè повеќе се спроведуваа надвор од територијата на НАТО, што не бараше големо вклучување на сојузничките ресурси за цивилна подготвеност. Префрлањето на неборбени основни воени задачи, барања и капацитети преку надворешни изведувачи стана норма.[60]

Дополнително, Пакетот за воена мобилност беше најавен во Белата книга за подготвеност на европската одбрана 2030[61] на 19 март 2025 година. Иницијативата ја нагласува посветеноста на Комисијата, заедно со онаа на Европската служба за надворешна акција (EEAS) и на Европската агенција за одбрана (EDA), за тесна соработка на координиран начин со земјите-членки за подобрување на воената мобилност преку инфраструктурни инвестиции и стратешки законодавни и незаконодавни мерки. Пакетот ќе опфати заедничка комуникација за воената мобилност, во комбинација со законски предлози за олеснување и поддршка на воената мобилност во ЕУ, вклучувајќи целни измени на постојното законодавство на ЕУ за подобро да се земат предвид потребите на воената мобилност. Дополнително, Воената мобилност е од витално значење за европската безбедност и одбрана и капацитетот да реагира на природни и вештачки предизвикани нарушувања. Силите на земјите-членки на ЕУ треба да бидат способни да го извршуваат воениот транспорт на опрема, стоки и патници во Унијата и преку нејзините надворешни граници, а воедно да го минимизираат и ублажат влијанието на таквиот транспорт врз цивилниот транспорт, како и да реагираат брзо и со доволен обем на кризи што избувнуваат на надворешните граници на ЕУ и пошироко. Покрај тоа, руската агресија врз Украина секој ден покажува колку е важно воената помош и снабдување да се префрлаат што е можно побрзо и непречено.[62]

За таа цел, предложената нова Регулатива за воспоставување рамка на мерки за олеснување на транспортот на воена опрема, стока и персонал низ Унијата (19.11.2025)[63]

[59] https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3, посетена на 21/3/2026
[60] https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3, посетена на 21/3/2026
[61] White Paper for European Defence – Readiness 2030, посетена на 21/3/2026, достапна на: https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en?filename=White%20paper%20for%20European%20defence%20%E2%80%93%20Readiness%202030.pdf,
[62] https://transport.ec.europa.eu/news-events/news/have-your-say-military-mobility-challenges-2025-09-17_en, посетена на 21/3/2026
[63]Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework of measures to facilitate the transport of military equipment, goods and personnel across the Union, 2025, посетена на 11/3/2026, достапна на: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0847,

и Заедничката комуникација до Европскиот парламент и Советот за воена мобилност[64] се во насока на воспоставување Зона за воена мобилност низ целата ЕУ до крајот на 2027 година како прв чекор кон постепено постигнување на „Воен Шенген“ во регулаторни, инфраструктурни и капацитетни димензии. Иако е постигнат важен напредок, значајните пречки за ефикасна воена мобилност во ЕУ продолжуваат да постојат. Различните национални правила, фрагментираните процедури и отсуството на јасна координација продолжуваат да го одложуваат воениот транспорт. Транспортната инфраструктура на ЕУ е недоволно прилагодена на потребите за двојна употреба и останува ранлива на прекини. Пристапот до горива за воени транспортни операции останува предизвик. Транспортните капацитети за двојна намена кои се критични за воените транспортни операции остануваат оскудни. Овие бариери ги откриваат критичните ранливости за транспортната мрежа на Унијата и го поткопуваат безбедносниот став на ЕУ, операциите за цивилна заштита и капацитетот за одвраќање. Комисијата предлага како дел од Регулативата рамка за вонредни состојби за прекугранично воен транспорт, Европски систем за подобрен одговор на воена мобилност (EMERS), кој ќе активира подобрена и координирана рамка за одговор за прекугранично воен транспорт во случај на вонредни состојби каде што стандардните процедури не се во согласност. Тој ќе овозможи привремени, вонредни мерки за да се гарантира подобрен прекугранично воен транспорт и приоритетен пристап за вооружените сили до инфраструктура, транспортни средства и основни услуги. Ќе вклучува унифицирани регулаторни процедури и правила, целни отстапувања и ослободувања, подобрени мерки за подготвеност и солидарност и зголемена отпорност на инфраструктурата.[65]

Иако Директивата за отпорност на критични субјекти (CER) утврдува хармонизирани барања за зголемување на отпорноста на критичните субјекти во ЕУ, инфраструктурата што е клучна за воената мобилност бара посебна заштита. За да се заштити дополнително, Комисијата предлага да се воспостави процес за земјите-членки да идентификуваат стратешка инфраструктура со двојна намена. Врз основа на заеднички пакет алатки од мерки за отпорност и заштита што одат подалеку од инструментите на Директивата CER, земјите-членки ќе можат да обезбедат дека стратешката транспортна, енергетска и комуникациска инфраструктура е отпорна на сите опасности и останува оперативна. Како што е најавено во Белата книга за одбранбена подготвеност, ова вклучува посилни мерки за ублажување на ризиците поврзани со странска сопственост или контрола на стратешката инфраструктура со

[64] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Military Mobility, 2025, посетена на 11/3/2026, достапна на: https://defence-industry-space.ec.europa.eu/document/download/a5b639aa-4d77-44b8-9f98-6bc0e54be984_en?filename=Joint%20communication%20on%20Military%20Mobility.pdf, посетена на 11/3/2026

[65] Исто.,стр.6

двојна намена, како и можноста земјите-членки привремено да преземат контрола врз важна инфраструктура, опрема и средства.[66]

Генерално, односите со НАТО за прашањата на воената мобилност ќе бидат зајакнати и ќе имаат меѓусебно корисно и трансформативно влијание за земјите-членки и сојузниците на НАТО кои не се членки на ЕУ.

3. Идентификација на каскадни ефекти меѓу секторите на критичната инфраструктура

Критичната инфраструктура (КИ) често има двојна намена и е од витално значење и за цивилни и за воени цели. Безбедното и стабилно снабдување со суровини, компоненти и стоки за широка потрошувачка е клучно за функционирањето на нашите економии и инфраструктура. Ова, исто така, игра клучна улога за одржување на воените операции, особено во олеснувањето на безбедното снабдување со опрема, материјал, делови за поправка и муниција од одбранбената индустриска база до првите линии. Изминатите неколку години го истакнаа степенот до кој критичната инфраструктура и безбедноста на снабдувањето се ранливи, без разлика дали се од природни или човечки предизвикани катастрофи (како пандемијата Ковид-19 или блокадата на Суецкиот канал во март 2021 година) или од намерно таргетирање (како што Русија го нанесе на енергетската и комуникациската инфраструктура на Украина).[67]

Нашите демократски општества и нашите економии се потпираат на критична инфраструктура, која обезбедува основни услуги на нашите граѓани и ги поткрепува нашите економии. Воените сили, исто така, во голема мера се потпираат на јавната и приватната цивилна инфраструктура за да можат да ги исполнат своите задачи.

Отпорноста на критичната инфраструктура на земјите-членки и сојузниците е првенствено национална одговорност. Отпорноста опфаќа способност за спречување, заштита, одговор, отпор, ублажување, апсорбирање, сместување и закрепнување од инциденти кои имаат потенцијал да го нарушат обезбедувањето основни услуги. Ова е особено важно за критичната инфраструктура бидејќи целосната заштита генерално не е можна. Инфраструктурата често ги преминува националните граници или обезбедува услуги што го прават тоа и затоа е неопходна соработката на регионално и меѓународно ниво, вклучително и преку меѓународни организации.

[66] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Military Mobility, 2025 , посетена на 11/3/2026, стр.9, достапна на https://defence-industry-space.ec.europa.eu/document/download/a5b639aa-4d77-44b8-9f98-6bc0e54be984_en?filename=Joint%20communication%20on%20Military%20Mobility.pdf, посетена на 11/3/2026, стр.9

[67] NATO RESILIENCE SYMPOSIUM, 25-27 APRIL 2023, RIGA, LATVIA,стр.12

Прекините на критичната инфраструктура можат да имаат значителни негативни последици за виталните владини функции, основните услуги за населението и економската активност на сојузничките и земјите-членки на ЕУ. Тие исто така можат да ги попречат воените активности, вклучувајќи вежби, распоредување, засилување и одржување. Покрај тоа, сложените меѓузависности значат дека нарушувањето на критичната инфраструктура може да има каскадни или меѓусебно засилувачки ефекти. На пример, нарушувањето на снабдувањето со електрична енергија може да влијае на јавните услуги и снабдувањето со витални добра. Ваквите последици може да ги преминат и границите, поради меѓусебните врски на мрежите и фактот дека во некои случаи самата инфраструктура се протега на повеќе од една земја.[68]

Критичната инфраструктура во многу случаи е во приватна сопственост, под приватна управа или управување. Бидејќи овозможува критични владини услуги и основни услуги за населението и економските актери, а во некои случаи служи и за безбедносна и одбранбена цел, владите мора да обезбедат дека е отпорна на нарушувања. Ова вклучува разгледување на инвестициите што може да бидат неопходни.[69]

Критичните инфраструктури, кои служат како основа на нашето модерно општество, се соочуваат со зголемени ризици од сајбер закани, физички напади и природни катастрофи. Дополнително, меѓузависностите меѓу критичните инфраструктури во текот на нивниот оперативен век можат значително да влијаат на нивниот интегритет и безбедност. Како резултат на тоа, подобрувањето на отпорноста на критичните инфраструктури се појави како врвен приоритет за многу земји, вклучително и Европската Унија. Ова вклучува не само разбирање на самите закани/напади, туку и стекнување знаење за областите и инфраструктурите што потенцијално би можеле да бидат засегнати. Проект финансиран од Европската Унија наречен PRECINCT (Подготвеност и спроведување на отпорност за каскадни сајбер-физички закани на критичната инфраструктура), во рамките на програмата Хоризонт 2020, се обидува да ги поврзе приватните и јавните засегнати страни на критичните инфраструктури во одредена географска област. Клучната цел на овој проект е да се воспостави заеднички пристап за управување со сајбер-физичката безбедност што ќе обезбеди заштита и на граѓаните и на инфраструктурите, создавајќи безбедна територија.[70]

Критичната инфраструктура е изложена на сè поголем ризик од разни намерни сајбер-физички напади и ризици од природни опасности. Сепак, проценката и

[68] EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE FINAL ASSESSMENT REPORT, JUNE 2023 стр.3
[69] Исто.,
[70] Gordan M., Kountche D.A., Resilient Cities and Structures, Protecting critical infrastructure against cascading effects: The PRECINCT approach, 2024, стр.1

справувањето со влијанието на каскадните ефекти што произлегуваат од меѓузависностите меѓу различните видови критични инфраструктури и различните видови опасности/закани и нивната отпорност за „брзо закрепнување“ станува сè порелевантно и исклучително тешко, особено во однос на одредени географски области како што се градовите. Зголемената ранливост на урбаните центри ја фокусира важноста на длабоката јавно-приватна соработка за да се обезбеди координиран мултисекторски одговор и подобрена заштита на критичната инфраструктура. Идентификацијата на различните влијанија од настан како што е поплава вклучува познавање на опасноста, регионот и инфраструктурите што ќе бидат засегнати. Современите критични инфраструктури се силно меѓусебно поврзани поради нивната зависност едни од други, стремежот кон ефикасност и оптимизација на ресурсите, потребата од размена на информации, економските размислувања, технолошкиот напредок и желбата за подобрување на услугите и корисничкото искуство. Затоа, ако една критична инфраструктура доживее намалено работење, тоа потенцијално може да влијае на другите во мрежата. Оттука, темелната анализа на заканите мора да ги земе предвид сите релевантни критични инфраструктури и нивните меѓузависности. [71]

Во согласност со Извештајот на работната група ЕУ-НАТО за отпорност на критичната инфраструктура од јуни 2023 година, секторската анализа истакнува дека секој сектор на основни услуги се потпира на специфична критична инфраструктура. Сепак, идентификувани се четири сектори од меѓусекторско значење кои обезбедуваат услуги што поддржуваат и овозможуваат други сектори: енергетика, транспорт, дигитална инфраструктура и вселена. Овие сектори се соочуваат со посебни предизвици на кои треба да се одговори со цел да се зајакне отпорноста. Енергетскиот сектор има специфични карактеристики кои бараат прилагодени мерки за да се обезбеди отпорност, имено:

- Потреби во реално време: некои енергетски системи треба да реагираат многу брзо, во некои случаи до милисекунди, и не дозволуваат дополнително време за обработка.

- Каскадни ефекти: ненадеен дефект во електричната мрежа може да предизвика брз домино ефект на дефекти, што може брзо да доведе до прекин на снабдувањето на голем број потрошувачи низ земјите и секторите.

[71] Исто.,стр.2-3

- Технолошки микс: застарената технологија и инфраструктура, со животен век од 30-60 години, ќе треба да се одржуваат истовремено со воведувањето на новите технологии и дигитализацијата.[72]

Постојат силни физички и дигитални меѓусебни врски што постојат меѓу секторите, вклучувајќи и други (на пример, јавно здравство, водоснабдување или земјоделство). Поради овој висок степен на меѓузависност помеѓу различните видови на инфраструктура, ефектите од нарушувањето во еден сектор можат да се шират каскадно, влијаејќи и на критичната инфраструктура во други сектори. Овие врски треба подобро да се разберат за да се предвидат потенцијалните каскадни ефекти, да се идентификуваат мерки за нивно ублажување и да се олесни ефикасен и комплементарен одговор преку цивилни и воени средства, вклучувајќи ги и оние достапни преку Механизмот за цивилна заштита на Унијата (UCPM). Брзорастечката дигитализација на секој од четирите сектори споменати погоре ги прави ранливи на злонамерни сајбер активности. Сајберпросторот е постојано оспоруван. Малициозните актери покажаа зголемена подготвеност да спроведат злонамерна сајбер активност против критична инфраструктура за да ги постигнат своите стратешки цели, вклучително и со спроведување обемно извидување; извршување напади, вклучително и против синџирите на снабдување; искористување на ранливостите во хардверот и софтверот; и искористување на лошата свест за сајбер хигиена и безбедност и во јавните и во приватните организации. Сопственоста или контролата од страна на потенцијалните противници врз критичната инфраструктура и поддржувачките синџири на снабдување во сојузниците и земјите-членки, исто така, претставува потенцијален предизвик. Ова би можело да овозможи пристап до податоци и информации или може да се искористи за деградирање, нарушување или одбивање на пристап или задржување на услуги. На пример, сопственоста или контролата на транспортната инфраструктура би можела да се искористи за добивање информации за воена опрема или операции или за отежнување или одложување на распоредувањата.[73]

4. <u>Заштита и отпорност на критичната инфраструктура</u>

Зајакнувањето на отпорноста и заштитата на критичната инфраструктура од сите видови закани во последните години влегува во сите сфери на безбедносните политики на бројни држави, акцентирајќи ја важноста на критичната инфраструктура како едно приоритетно безбедносно прашање.

[72] EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE FINAL ASSESSMENT REPORT, JUNE 2023, стр.5-6
[73] Исто., стр.8

Невозможно да се заштити целата критична инфраструктура од сите закани и опасности, цело време.

Безбедност на инфраструктурата подразбира заштита на оние инфраструктури што се перцепираат како критични, како што се аеродромите, автопатишта, болници, мостови, транспортни јазли, мрежни комуникации, медиуми, мрежи за снабдување со електрична енергија, брани, нуклеарни електрани, пристаништа, рафинерии за нафта, водни системи итн. Главна цел на заштита на критичната инфраструктура е ограничување на ранливоста на конкретната инфраструктура, спречување на саботажи, тероризам и контаминација, како и спречување на ширење на негативни ефекти на одредено поголемо подрачје и на поголем број сектори, во случај на одреден настан со што би се прекинало нормалното функционирање на инфраструктурата.[74]

Во новата безбедносна средина, хибридните закани се најчесто насочени кон критичната инфраструктура, која како безбедносен и оперативен термин е релативно нова појава и особено се актуелизираше по рускиот напад врз Украина, опфаќајќи најчесто енергетски и транспортни системи, но и системи за водоснабдување, како и сообраќајна инфраструктура. Иако терминот е нов, тоа не значи дека критичната инфраструктура претходно не постоела. Напротив, секој општествен поредок во секое доба од човековиот развој имал некаква сопствена критична инфраструктура, односно системи есенцијални за општественото функционирање- водоснабдување, производство и снабдување со храна, определени патни коридори. Во променетата безбедносна средина, критичната инфраструктура е легитимен објект на заштита кој мора да биде препознаен од системот како таков преку императивот на нормата, односно правната рамка. За да може да ја заштитиме критичната инфраструктура, но и да се заштитиме, најпрвин, таа мора да биде препознаена од националното законодавство.[75]

Безбедноста на критичната инфраструктура е под закана од два фактора. Првиот е природниот фактор и тука спаѓаат опасностите од земјотреси, пожари, поплави, епидемии и сл., и вториот фактор што се однесува на намерното предизвикување штети (кражби, вандализам, тероризам итн). Отткука, заканите за критичната инфраструктура, може да бидат вештачки, како резултат на тероризам или други криминални активности, но може да бидат и природни, предизвикани од временските услови, како што се бури, вулкански ерупции, поплави или други еколошки катастрофи. Исто така, критичната

[74] О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура, Комора на Република Македонијаза приватно обезбедување 2017,стр.79, достапно на: https://obezbeduvanje.org.mk/wp-content/uploads/2020/12/Zashtita-na-kriticna-infrastruktura-za-web.pdf, , посетено на 16/2/2026

[75] Попоска В., ИНФОРМИРАНА ОДБРАНА, Вовед за хибридните закани за критичната инфраструктура, Информативна студија, Што се хибридни закани, а што критична инфраструктура и како изгледа новата безбедносна архитектура?, Скопје 2024, стр.4

инфраструктура може да биде загрозена и од болести, пандемии и да влијае врз голем број критичен персонал.[76]

Критичната инфраструктура е широко распространета (често помеѓу неколку нации), во голема мера во сопственост и/или управувана од приватниот сектор, во многу случаи лесно достапна и зависна од глобалните синџири на снабдување. Глобалните синџири на снабдување генерално се дизајнирани според економски и практични размислувања, а не имајќи ги предвид отпорноста и редундантноста. Критичната инфраструктура, исто така, вклучува нематеријални услуги, како што се податоците потребни за балансирање на електричната мрежа и техничарите потребни за одржување на витална опрема. Услугата што ја обезбедува критичната инфраструктура мора да остане финансиски одржлива, што значи дека силните одбранбени мерки често се недостапни. Покрај тоа, компаниите надвор од НАТО можат да играат улога во финансирањето, изградбата или управувањето со критична инфраструктура, додавајќи дополнителни слоеви на сложеност. Затоа, иако приватниот сектор е клучен засегнат чинител и партнер во обезбедувањето и отпорна критична инфраструктура и отпорни синџири на снабдување, безбедноста не е нивна примарна мотивација. Сојузниците и организациите како НАТО можат да помогнат во обезбедувањето поголема свест за потенцијалните безбедносни загриженост и да покажат како правењето на поотпорна критична инфраструктура може да ги намали шансите за прекини, да ги минимизира негативните ефекти кога ќе се случат прекини и да обезбеди брзо продолжување на услугите потоа. Ова ја нагласува важноста на двонасочната јавно-приватна соработка. Фокусот треба да биде на зајакнување на отпорноста на инфраструктурната мрежа, а не само на заштитата на поединечните компоненти. Во овој контекст, стратешката соработка НАТО-ЕУ е единствена и суштинска. Силната улога на ЕУ во воспоставувањето релевантно законодавство кое ги обликува одлуките и планирањето на нејзините земји-членки и приватниот сектор придонесува за зајакнување на отпорноста на комплементарен начин во однос на НАТО.[77]

Отпорноста е национална одговорност и колективна обврска вкоренета во Член 3 од Северноатлантскиот договор.[78] Во обврската за зајакната отпорност, шефовите на држави и влади се согласија да усвојат поинтегриран и подобро координиран пристап за намалување на ранливостите и обезбедување дека нивните војски можат ефикасно да дејствуваат во мир, криза и конфликт.[79] Според НАТО 2030, шефовите на држави и влади, исто така, се обврзаа да развијат предлог за утврдување, проценка, преглед и следење на целите за отпорност за да ги водат национално развиените цели за отпорност

[76] О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура, Комора на Република Македонијаза приватно обезбедување 2017, стр.24
[77] NATO RESILIENCE SYMPOSIUM, 25-27 APRIL 2023, RIGA, LATVIA, стр.12
[78] NATO 2022 Strategic Concept; параграф 26.
[79] Strengthened Resilience Commitment; параграф 5

и планови за имплементација.[80] На Самитот во Мадрид во 2022 година, лидерите на НАТО го одобрија предлогот за продолжување на развојот на целите за отпорност за да ги водат националните цели и планови. Со исполнувањето на оваа задача, сојузниците се согласија да воспостават циклус на планирање и преглед за отпорност преку цивилна подготвеност, одделен, но координиран со Процесот на планирање на одбраната на НАТО.[81]

Иако заштитата и еластичноста на критичната инфраструктура се комплементарни концепти, мораме да ги објасниме и прифатиме разликите меѓу нив. Накратко, заштитата се однесува на способноста да се спречат или намалат ефектите од непријатни и ненадејни настани, додека еластичноста е олицетворена во способноста да се намали големината, влијанието и времетраењето на прекинот во функционирањето и се однесува на брз пристап кон сите компоненти и процеси, од физички компоненти до капацитетот за управување, како и квалитетот на човечките ресурси. Притоа, еластичноста тежнее кон развој и одржување на системот и неговата способност да се спречи, апсорбира, адаптира и да закрепне по секаков можен напад.[82]

Крајната цел на заштита на критичната инфраструктура е постигнување на соодветни безбедносни и заштитни потребни нивоа создавајќи континуитет на функционалноста на критичната инфраструктура. Со оваа фундаментална цел, важно е да се обезбеди процесот на опоравување во случај на деградација/катастрофа на функционалноста на системот. Идентификуваните и поставените компоненти на инсталираниот систем мора да го издржат влијанието на сите закани и ризици. Имајќи го предвид претходно наведеното, можеме да констатираме дека оптималното ниво на заштита на критичната инфраструктура претставува комбинација од: систем на физичка заштита; информатичка безбедност; планирање/управување со бизнис-сектор; административни процедури за безбедност и безбедносни мерки за вработените.[83]

Ефективната стратегија за заштита на критичната инфраструктура главно почива врз два столбови: ефективен систем за рано предупредување и ефективно менаџирање со кризи. Успешното функционирање на овие два системи придонесува кон мерките за намалување на ризикот, со што, пак, се зголемува безбедноста на критичната инфраструктура. Ефекивната стратегија за заштита на критичната инфраструктура во тој контекст треба да обезбеди ефективна проценка на ризикот и соодветна рамка за

[80] НАТО документ: PO(2021)0166-FINAL, NATO 2030 - A Transatlantic Agenda for the Future; параграф 11.a.
[81] НАТО документ: PO(2022)0037, Establishing Resilience Objectives and Nationally-developed Resilience Goals
[82] Митревска М., Милески Т., КОН ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА: СТУДИЈА НА СЛУЧАЈ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА, Фондација „Фридрих Еберт“, 2022, стр.156
[83] О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура, Комора на Република Македонијаза приватно обезбедување 2017, стр.29

дејствување. Опасноста од други субјекти кои имаат мрежна и глобална поставеност, но и од потенцијални природни катастрофи, во услови на голем број субјекти (од јавен и приватен сектор, со различни интереси, а истовремено меѓусебно зависни во доменот на давањето услуги), ја наметнува потребата од централизиран начин на одлучување. Централизираниот начин на донесување одлуки, колку и да изгледа, на прв поглед, старомодно и либерално е неопходен заради две причини: Прво, преку него се обезбедува ефективна координација во доменот на раното предупредување. Сите инволвирани актери добиваат неопходни информации за состојбата со потенцијалната опасност од природни катастрофи. Второ, со централизираниот начин на донесување одлуки сите актери применуваат ист пакет на мерки и стандарди.[84]

5. Транснационални размислувања за заштита на критичната инфраструктура

Тенденцијата последиците од нарушување на нормалното функционирање на инфраструктурата на земјата да се чувствуваат и надвор од границите на одредена држава, доведе до воведување нов термин − транснационална инфраструктура, што ги означува оние инфраструктури што ги поврзуваат државите. Денес, може да се зборува за сè поголем број инфраструктурни сектори што се трансформираат во транснационални – секторот за информатичка и комуникациска технологија одамна ги надмина националните граници на државите (а од ден на ден станува сè повлијателен), а исто така, транснационални се секторите за транспорт (патен, железнички, воздушен, воден), телекомуникацискатa, хемискатa индустрија, како и нуклеарната индустрија. Особено значаен е и финансискиот сектор, кој дефинитивно во голема мера е транснационален.[85]

Кога една земја-членка идентификувала потенцијална критична инфраструктура на територијата на други земји-членки или открила дека има своја инфраструктура на нејзината територија што е значајна за соседните земји, таа истите е задолжена да ги информира за тој податок. Се разгледува само инфраструктурата која е од суштинско значење за одржување на виталните функции на општеството, здравјето, сигурноста, безбедноста и економската или социјалната благосостојба на луѓето, а чие нарушување или уништување би имало значително влијание врз една или две земји членки. Потоа, следи процес на билатерални или мултилатерални дискусии меѓу државите со цел да се разгледаат состојбите и потенцијалните негативни ефекти од застојот или дефектот во работењето на утврдената инфраструктура. На покана на земјите членки, Европската комисија може да учествува во овие дискусии. По извршената анализа, за да се

[84] Попоска В., ИНФОРМИРАНА ОДБРАНА, Вовед за хибридните закани за критичната инфраструктура, Информативна студија, Што се хибридни закани, а што критична инфраструктура и како изгледа новата безбедносна архитектура?, Скопје 2024, стр.11

[85]О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура, Комора на Република Македонијаза приватно обезбедување 2017, стр.стр.81

идентификува потенцијалната критична инфраструктура како европска критична инфраструктура, потребна е согласност од земјата членка на чија територија е откриена и назначена како европска критична инфраструктура. Во случај на неможност да се постигне договор меѓу земјите членки, тие можат да се обратат до Комисијата, која може да се вклучи во дискусијата и да го олесни постигнувањето на договор меѓу државите. По успешните преговори меѓу земјите членки, следниот чекор е да се информираат сопствениците или операторите на критичната инфраструктура дека нивната инфраструктура е идентификувана и означена како европска критична инфраструктура. Земјата членка на чија територија се наоѓа оваа европска критична инфраструктура е одговорна за информирање на сопственикот или операторот и исто така е должна на годишно ниво да ја известува Комисијата за бројот на означени европски критични инфраструктури по сектор и за бројот на земји членки кои зависат од секоја означена европска критична инфраструктура.[86]

Увидот во сите релевантни и на меѓународно ниво значајни транснационални инфраструктури во Европа беше постигнат со формирање листа на критична инфраструктура на Европската унија. Всушност, еден од предусловите одредена инфраструктура да е од клучно значење на ниво на ЕУ е да биде транснационална, односно последиците од нејзино откажување да се почувствуваат не само во земја каде што има прекин на функционирањето, туку барем и во друга земја. Слични правила и прописи постојат на ниво на сите организации што имаат транснационален карактер, а се занимаваат со прашањата за поефикасно користење и заштита на инфраструктурата. Новите размислувања одат во насока дека комплексните инфраструктурни системи е потребно да се разгледуваат како отворени, ранливи системи со многу внатрешни проблеми.[87]

Денес експертите во областа на заштитата на критичната инфраструктура повеќе ја практикуваат оваа концепција на критична инфраструктура, а со оглед на фактот дека заштитата на критичната инфраструктура не се гледа само како на заштита од надворешни напади, туку под овој концепт се подразбира и планирање на обновувањето, кој е важен индикатор на успешната политика на заштита на критичната инфраструктура за да може системот да функционира во сите услови и да може брзо да закрепне во случај на оштетување на одреден сегмент на критичната инфраструктура.

ГС на НАТО Руте во своето обраќање на НАТО Симпозиумот за отпорност што се одржа во Словачка во ноември 2024 го истакна значителниот напредок што НАТО и

[86] Митревска М., Милески Т., КОН ОТПОРНОСТ И ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА: СТУДИЈА НА СЛУЧАЈ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА, Фондација „Фридрих Еберт“, 2022, стр.66

[87] О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура, Комора на Република Македонијаза приватно обезбедување 2017, стр.82

поединечните сојузници го постигнаа од 2014 година за зајакнување на отпорноста - сè поважна задача, бидејќи општествата на земјите членки на НАТО се соочуваат со растечки предизвици, без разлика дали станува збор за катастрофи поврзани со климата или малигни сајбер активности. Во контекст на НАТО, отпорноста е способност за подготовка, спротивставување, реагирање и брзо закрепнување од шокови или нарушувања и е приоритет и за сојузниците и за партнерите. Генералниот секретар истакна дека отпорноста не е строго воена или цивилна, туку „одговорност на целата влада и целото општество“. Затоа сојузниците одлучија да го интегрираат цивилното планирање во националното и колективното одбранбено планирање. ГС Руте истакна дека иако овој напредок е важен, има уште работи што треба да се направат, нагласувајќи ја „потребата да се удвои градењето заедничка култура на отпорност низ евроатлантскиот регион“, додека се гради заедница на НАТО што ги вклучува јавниот и приватниот сектор, заедно со други меѓународни организации, особено Европската Унија. „Заедно, можеме подобро да се спротивставиме на растечкиот притисок од оние кои сакаат да ги искористат нашите ранливости“, заклучи генералниот секретар во своето обраќање.[88]

Со оглед на зависноста од критичната инфраструктура за обезбедување основни услуги и за цивилното население и за воените сили, таквата инфраструктура треба да биде отпорна и способна да издржи нарушувања. НАТО и сојузниците ги засилија своите напори во оваа област, вклучително и преку размена на најдобри практики.

Подморските кабли носат околу 10 трилиони американски долари трансфери секој ден; две третини од светската нафта и гас се вадат на море или се транспортираат по море; а околу 95 проценти од глобалните текови на податоци се пренесуваат преку подморски кабли. За НАТО, заштитата на критичната подморска инфраструктура е од суштинско значење за безбедноста и одбраната, бидејќи е клучна за обезбедување и заштита на просперитетот на сојузничките општества.[89]

Како одговор на саботажата на цевководите „Северен поток“ во 2022 година, сојузниците на НАТО значително го зголемија своето воено присуство околу клучната инфраструктура, вклучително и со бродови и патролни авиони, како и поставија „Координативна ќелија за критична подморска инфраструктура во седиштето на НАТО“ со намера да се подобри безбедноста на „високо ранливите подморски кабли и цевководи“. [90]

[88] https://www.nato.int/en/news-and-events/articles/news/2024/11/12/secretary-general-addresses-the-2024-nato-resilience-symposium, посетена на 16/2/2026
[89] https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3, посетена на 16/2/2026
[90] Andersen, L. H., Broeders D, Protecting Transnational Information Infrastructure: Vitality, Vulnerability and Diplomacy. Policy brief, EU Cyber Direct, 2023, стр.20

Обезбедувањето отпорност на инфраструктурата што е критична за земјите-членки на ЕУ и сојузниците на НАТО е важен елемент на стратешкото партнерство и соработката меѓу двете организации, имајќи ја во предвид зголемената комплексност на безбедносните закани. Во таа насока, претседателот на Европската комисија и генералниот секретар на НАТО на 11 јануари 2023 година, објавија формирање на посветена работна група НАТО-ЕУ за отпорност на критичната инфраструктура. Работната група ЕУ-НАТО е целосно вградена во постојниот структуриран дијалог НАТО-ЕУ за отпорност и дополнително го зајакнува со целосно почитување на договорените водечки принципи содржани во трите заеднички декларации за соработка меѓу ЕУ и НАТО. Извештајот ја опишува важноста на критичната инфраструктура, го проценува моменталниот безбедносен контекст карактеризиран со зголемено ниво на ризик и истражува четири клучни сектори: енергетика, транспорт, дигитална инфраструктура и вселена, како и меѓусекторски размислувања. Извештајот презентира конкретни препораки за активности што би можеле да придонесат за зајакнување на отпорноста на критичната инфраструктура, во поддршка на земјите-членки на ЕУ и сојузниците на НАТО.[91]

На самитот на НАТО во Вилнус во 2023 година, шефовите на држави и влади на сојузничките земји ја истакнаа реалната и растечката закана за критичната подморска инфраструктура, која игра важна улога во отпорноста на сојузниците. Тие се согласија да го основаат Поморскиот центар на НАТО за безбедност на критичната подморска инфраструктура во рамките на Поморската команда на НАТО во Обединетото Кралство. Тие, исто така, се согласија да формираат мрежа што ги обединува НАТО, сојузниците, приватниот сектор и други релевантни актери за подобрување на споделувањето информации и размена на најдобри практики. Подобрувањето на безбедноста на критичната подводна инфраструктура е од суштинско значење за колективната одбрана и отпорност на НАТО. Овие витални системи ја поткрепуваат глобалната комуникација, трговијата и снабдувањето со енергија, што значи дека нивната одбрана е стратешки приоритет. За да го поддржи Центарот, НАТО, исто така, воспостави Мрежа за критична подводна инфраструктура која ги опфаќа сојузниците, приватниот сектор и други релевантни актери за да се олесни споделувањето информации и размената на најдобри практики.Технологијата игра клучна улога во заштитата на подморската инфраструктура, а НАТО продолжува да промовира иновации - како што се морски дронови, сензори и употреба на вештачка интелигенција - за откривање на сомнителни активности на море.[92]

[91] EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE FINAL ASSESSMENT REPORT, JUNE 2023, стр.2

[92] https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3, посетена на 16/2/2026

Нарушувањата на критичната инфраструктура, поради сè повеќе испреплетената и поврзана економија и општества, можат да имаат значителни последици низ секторите и границите. Нарушувањата на критичната инфраструктура можат да дојдат од многу извори, и природни и предизвикани од човекот.

Јавните простори, но и критичните инфраструктури се стратешки цели за терористите, доколку јавните простори можат да концентрираат значителен број луѓе, и дека нападот врз критичните инфраструктури како што се електричните мрежи, транспортните мрежи и водоснабдувањето може да го наруши и измени виталното функционирање на основните услуги. Во овој контекст, проценката на ризикот од тероризам може да го процени потенцијалното влијание, сериозноста и веројатноста за појава на терористички напади, преку интервенции во различни фази, вклучувајќи превенција, ублажување, подготвеност, закрепнување и реконструкција или адаптација.

Загрозеноста на критичната инфраструктура од хибридни закани, најмногу се должи на фактот што генерално критичната инфраструктура претставува т.н. „мека цел“. Поимот „меки цели»10 најчесто се поврзува со места каде што се собираат луѓето во голем број, како што се музеи, кина, религиозни локации, трговски центри и слично. Меките цели се контрастни со т.н. „тврди цели“, кои широко ги идентификуваат местата каде што обезбедени се високи нивоа на заштита, често од вооружени лица, односно локации каде пристапот на јавноста е ограничен или подлежи на тешки контроли (на пример, воени инсталации). Конечно, можеби критичната инфраструктура претставува мека цел, но, сите меки цели не се критична инфраструктура. Клучниот елемент за разликување се однесува на прашањето на „критичност». Меките цели не мора да изгледаат како критични за обезбедувањето на основните општествени услуги. Такви се, на пример, стадионите и концертните хали.[93]

5.1 НАТО и ЕУ соработка во зајакнување на отпорноста на критичната инфраструктура и соработката со партнерите

ЕУ и НАТО имаат заеднички интерес да спречат нарушувања на критичната инфраструктура што обезбедува основни услуги за граѓаните и ги поддржува нашите економии. Двете организации ќе продолжат да соработуваат на комплементарен и меѓусебно зајакнувачки начин за да изградат отпорност и да бидат подготвени да управуваат со нарушувања од кој било извор. Како придонес кон работата на Работната група НАТО-ЕУ, Ќелијата за хибридна фузија на ЕУ и Одделот за хибридна анализа, Одделот за производство на разузнавачки податоци на Заедничката дивизија за разузнавање и безбедност на НАТО спроведоа Паралелна и координирана проценка

[93] Попоска В., ИНФОРМИРАНА ОДБРАНА, Вовед за хибридните закани за критичната инфраструктура, Информативна студија, Што се хибридни закани, а што критична инфраструктура и како изгледа новата безбедносна архитектура?, Скопје 2024, стр.4

(Parallel and Coordinated Assessment - PACA) на пејзажот на закани поврзани со критичната инфраструктура, во согласност со утврдената практика на соработка НАТО-ЕУ. НАТО и ЕУ ги поддржуваат своите членки со насоки, олеснуваат размена на најдобри практики, спроведуваат вежби, обезбедуваат ресурси и нудат комплементарни алатки за градење отпорност. Земјите-членки на ЕУ и сојузниците на НАТО се охрабруваат да ги користат максимално. [94]

Штабовите на НАТО и ЕУ ги идентификуваа следните препораки за градење на нивната соработка:

1. Обезбедување брз ангажман помеѓу високите претставници на ЕУ и НАТО во случај на идентификувана голема опасност за критичната инфраструктура или значителна промена во безбедносниот контекст;

2. Развивање редовни паралелни и координирани проценки на заканите за критичната инфраструктура, надоградувајќи ја онаа спроведена пролетта 2023 година;

3. Зајакнување на структурираниот дијалог за отпорност и структурираниот дијалог за воена мобилност, и проширување на постојните разговори на штабот за кибернетика, вселена, поморство и енергија, како и помеѓу Меѓународниот воен штаб на НАТО и Воениот штаб на ЕУ, со цел:

а) Продлабочување на разбирањето на релевантните алатки и процеси што се достапни за секоја организација;

б) Анализирање на набљудувањата од агресивната војна на Русија против Украина во врска со отпорноста на критичната инфраструктура;

в) Понатамошно анализирање и спроведување на подлабока проценка на импликациите врз безбедноста на критичната инфраструктура на релевантните синџири на снабдување, енергетската транзиција и новите технологии.

4. Целосно искористување на синергиите помеѓу соодветните процеси што произлегуваат од политиките и програмите на ЕУ и НАТО за критична инфраструктура, вклучително и преку редовни вкрстени брифинзи до Групата за отпорност на критичните субјекти на ЕУ и Политичко-воената група, како и Комитетот за отпорност на НАТО;

[94] EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE FINAL ASSESSMENT REPORT, JUNE 2023, стр.4.

5. Систематско земање предвид на отпорноста на критичната инфраструктура во сите идни паралелни и координирани вежби;

6. Одржување на наменски дискусии базирани на сценарија помеѓу штабовите за подобро разбирање на предизвиците, меѓузависностите и каскадните ефекти, вклучително и преку Семинарот за предвидување ЕУ-НАТО и со поддршка на Европскиот центар за извонредност за справување со хибридни закани;

7. Подобрување на свеста за безбедносните импликации од учеството или контролата на критичната инфраструктура од страна на субјекти од стратешки конкуренти, како и потенцијалните ризици поврзани со добавувачите од тие земји, вклучително и во 5G мрежите;

8. Истражување на можностите за размена на мислења за тоа како да се подобри следењето и заштитата на критичната инфраструктура во поморската област од страна на надлежните органи и дискусија за начините за подобрување на свеста за поморската ситуација;

9. Промовирање на размена на најдобри практики меѓу цивилните и воените актери за спроведување на релевантни политики и Закони поврзани со сајбер, вклучително и за релевантното законодавство насочено кон подобрување на сајбер-отпорноста на критичната инфраструктура за поотпорна војска;

10. Размена на најдобри практики за подобрување на отпорноста на критичната инфраструктура и идентификување на потенцијални начини за нејзино понатамошно зајакнување, на пример преку проценка на потребата, релевантноста и изводливоста на специфичните барања за одредена транспортна инфраструктура со цел да се прилагоди на тежината, големината или размерот на воениот транспорт;

11. Идентификување на алтернативни транспортни правци и за цивилни и за воени цели во случај на значително прекинување на одредена рута;

12. Промовирање на ангажманот меѓу сојузниците, земјите-членки и приватниот сектор, вклучително и за безбедноста преку дизајн за критична инфраструктура;

13. Промовирање на размена за управување со меѓусекторските последици од големите пречки на критичната инфраструктура, особено преку зголемена соработка меѓу НАТО и Координативниот центар за одговор во итни случаи (ERCC) на ЕУ.

14. Идентификување на синергии и потенцијални области на соработка во активностите за истражување на безбедноста поврзани со критичната инфраструктура, вклучувајќи ги

и предизвиците поврзани со новите технологии или безбедноста на синџирот на снабдување. [95]

Дополнително, за зајакнување на отпорноста на критичната инфраструктура големо значење има и Механизмот за скрининг на странски директни инвестиции, кој е предвидено да биде решение за проблемот наречен „корозивен капитал“. Овој механизам е во вид на државни мерки насочени кон странски инвестиции кои се однесуваат на одредени категории од националната економија, преку ограничување или забрана на странските директни инвестиции да влезат на нејзината територија.[96]

Како резултат на сеопфатната анализа на структурата на странските директни инвестиции, користа која ја носат со себе, но и ризиците исто така, Европската комисија ја предложи (2019), а Советот на ЕУ ја усвои, Регулативата за воспоставување на координативен механизам за проверка (скрининг) на странските директни инвестиции (СДИ)[97] на целата територија на Европската Унија. Регулативата влезе во сила од октомври 2020 година и таа претпоставува дека како прво ниво на проверка секоја земја членка на ЕУ има воспоставен целосно функционален национален систем (правен и институционален) за скрининг на странските директни инвестиции, вклучително и спојување и купување на домашни компании со странски капитал. Второто ниво на проверка на СДИ е токму ЕУ-координативниот механизам кој наметнува задолжителна размена на информации меѓу земјите членки и Европската комисија низ сигурни криптирани канали на комуникација кои ќе обезбедат доверба кај економските оператори за споделување на сите потребни информации и избегнување на секаков вид потенцијални злоупотреби. Примарна цел на интерес при скринингот на инвестициите се вложувањата во критичната инфраструктура, како и секторите кои се од осетлива природа, и тоа пред сè енергетика, транспорт, ИТК, здравство, одбрана, медиуми, финансиската и изборната инфраструктура, технологиите за мониторинг над сајбер просторот, па дури и учеството во програмите на Унијата кои се финансирани од страна на ЕУ-фондовите како што се Галилео, Коперникус, Хоризонт 2020, ПЕСКО итн[98].

Насоките на Европската комисија се дека сите земји членки, и оние кои претендираат да станат членки, односно се во процес на пристапни преговори, треба да имаат на време воспоставен целосно функционален национален систем за проверка на

[95] Исто,. стр.8-9
[96] Јовановски З., Мизо В., Тилев Д., Механизам за скрининг на странски директни инвестиции во Северна Македонија - Зошто и како?, Студија за политика, 2022, стр.8
[97] REGULATION (EU) 2019/452 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452, посетена на 1/3/2026
[98] ANNEX List of projects or programmes of Union interest referred to in Article 8(3), REGULATION (EU) 2019/452 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

странските директни инвестиции, кој ќе биде способен да комуницира со националните системи на земјите членки на ЕУ, но и со стручните служби на Европската Комисија.

По предлогот на Европската комисија за нова регулатива за скрининг на СДИ во ЕУ во јануари 2024 година, Европскиот парламент усвои изменета верзија на Нацрт-регулативата на 8 мај 2025 година. Советот ја усвои неговата изменета верзија на 11 јуни 2025 година. Европската комисија, Европскиот парламент и Советот моментално се вклучени во трилогијата за да се договорат за конечниот текст кој, откако ќе биде одобрен од Европскиот парламент и Советот, ќе означи клучен чекор во ревизијата на рамката за странски директни инвестиции на ЕУ. Иако трите институции на ЕУ имаат различни пристапи во своите нацрт-текстови, нивната заедничка намера е да ја укинат и заменат Регулативата од 2019 година за да ја подобрат нејзината ефикасност и ефективност и да промовираат поголема хармонизација меѓу земјите-членки. Оваа реформа, исто така, одговара на променливиот геополитички пејзаж и зголемената загриженост за стратешките зависности и странското влијание во критичните области. Според новите правила, повеќе сектори, како што се медиумските услуги, критичните суровини и транспортната инфраструктура, ќе бидат предмет на задолжителна проверка од страна на земјите-членки, со цел да се идентификуваат и да се справат со ризиците поврзани со безбедноста или јавниот ред поврзани со странските инвестиции. Одразувајќи го овој поширок стратешки контекст, Нацрт-регулативата го проширува опсегот на скринингот на странски директни инвестиции надвор од јавната безбедност и јавниот ред за да ја вклучи и заштитата на економската безбедност на ЕУ. [99]

Тоа претставува важен чекор кон зајакнување на безбедноста и јавниот ред на ЕУ, осигурувајќи дека странските инвестиции ќе продолжат да ја поддржуваат, а не да ја поткопуваат, економската безбедност, отпорноста и поширокиите интереси на Европа. Ревидираната рамка ќе го направи скринингот на инвестициите поробусен, кохерентен и стратешки. Ќе ја зајакне способноста на ЕУ да идентификува и колективно да се справи со потенцијалните ризици од странски инвестиции за безбедноста и јавниот ред.[100]

[99] https://www.europarl.europa.eu/legislative-train/carriage/revision-of-the-fdi-screening-regulation/report?sid=9901, посетена на 1/3/2026

[100] https://policy.trade.ec.europa.eu/news/revision-eus-foreign-investment-screening-mechanism-2025-12-11_en, посетена на 31/3/2026

ГЛАВА III

Стратешки комуникации

Стратешката комуникација (StratCom) претставува „холистички пристап кон комуникацијата, базиран на вредности и интереси, кој опфаќа сè што прави еден актер за да постигне цели, во контроверзна средина“. Опфаќа „долгорочни, сложени решенија и ефикасни начини за влијание врз големи, важни дискурси во многу конкурентна средина“ и обезбедува кохерентност на стратешкото влијание преку стремеж кон разбирање на клучните публики и обезбедување конзистентно планирање. Овој пристап ја смета комуникацијата не како средство за пренесување стратегија, туку како стратегија сама по себе.[101]

Во спротивставувањето на хибридните закани, стратешките комуникации се посебна област на НАТО-ЕУ соработката каде е постигнат значителен напредок. Градејќи заедничка култура на соработка во стратешките комуникации, Штабовите на ЕУ и НАТО постојано разменуваат сознанија во реално време, анализи, соодветни комуникациски планови, како и извештаи за манипулација и мешање со странски информации, вклучително и дезинформации. Една од целите во областа на стратешките комуникации е да се има заедничка порака и наратив за безбедносните закани и заеднички контакт со трети земји.

1. НАТО-ЕУ соработка во стратешките комуникации

Во однос на одговорот на НАТО на хибридни закани и дезинформации, беа донесени две важни одлуки: да воспостави стратешки комуникациски способности во седиштето на НАТО и да иницира формирање на Центар за извонредност на НАТО за стратешки комуникации во Рига. Вежбите за управување со кризи на НАТО почнаа да вклучуваат хибридни сценарија кои опфаќаат дезинформации, закани за критичната инфраструктура и ситуации во „сивата зона“ – просторот и времето помеѓу војната и мирот. Специјалниот координатор за хибридни закани - позиција создадена во 2025 година - служи како фокусна точка на високо ниво за целата работа на НАТО за борба против хибридните закани и обезбедува одговорот на НАТО на хибридните закани да остане силен, ефикасен и кохерентен. Сегашниот специјален координатор е помошникот

[101] Klingová K.,From Words to Action: Best Practices in Strategic Communication, GLOBSEC, 2024 https://www.globsec.org/what-we-do/publications/words-action-best-practices-strategic-communication, посетена на 22/3/2026

генерален секретар за сајбер и дигитална трансформација, Жан Чарлс Елерман-Кингомбе. [102]

Соработка за справување со хибридните закани во годините по Заедничката декларација на ЕУ и НАТО во 2016 година, 2018 година и 2023 година, променетата безбедносна средина и желбата за пристап до меѓусебните ресурси ја одржаа соработката меѓу ЕУ и НАТО во подобластите на ситуациска и информатичка свест и стратешките комуникации и доведоа до воспоставување на Европскиот центар за извонредност за справување со хибридни закани во Хелсинки (Hybrid CoE), кој делува како фасилитатор организирајќи работилници за стратешките комуникации за персонал од ЕУ и НАТО. Дополнително, веб-страницата „EUvsDisinfo.eu“ на ЕУ и акаунтите на социјалните медиуми се користат за разоткривање на дезинформациите не само за ЕУ, туку и за НАТО. НАТО е додаден и во Системот за брзо предупредување на ЕУ кој го олеснува размената информации меѓу земјите-членки на ЕУ во врска со новите или тековните кампањи за дезинформации: Заедничката информативна средина се споменува при обликувањето на прес-документите и како резултат на тоа пораките од ГС на НАТО и Претседателот на ЕК се исти. Кога делегации од трети земји го посетуваат седиштето на двете организации во Брисел, персоналот што работи на стратешки комуникации од ЕУ и НАТО работи заедно за да создаде заеднички пораки и наративи.

2. Дезинформациите како хибридни закани

Во современиот глобализиран свет информацијата претставува моќна алатка што може да биде искористена како инструмент за влијание врз општествата, политичките процеси и безбедносните политики. Иако информациското војување не е нова закана, напредната технологија им овозможи на злонамерните актери подобро да го користат информациското војување како дел од геополитичките стратегии.

Дезинформациите не се само ширење на неточни информации, туку имаат намера да измамат и се шират со цел да нанесат сериозна штета. Дезинформациите можат да ги шират државни или недржавни актери. Тие можат да влијаат на широк спектар на човекови права, поткопувајќи ги одговорите на јавните политики или засилувајќи ги тензиите во време на вонредна состојба или вооружен конфликт. Не постои универзално прифатена дефиниција за дезинформации. Ниту една дефиниција не може да биде доволна сама по себе, со оглед на повеќекратните и различни контексти во кои може да се појават загрижености во врска со дезинформациите, вклучително и во однос на

[102] https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats, посетена на 21/2/2026

прашања толку разновидни како што се изборниот процес, јавното здравство, вооружените конфликти или климатските промени. [103]

Информативните закани, како што се дезинформациите, го кинат ткивото што ги држи општествата заедно. Тие ја поткопуваат довербата на луѓето во владите и другите јавни институции. Тие обично се дизајнирани да се привлечат на најлошите импулси, стравови и предрасуди на луѓето - спротивставувајќи ги соседите, труејќи ги социјалните групи едни против други, потврдувајќи и разгорувајќи го екстремизмот, деградирајќи ги чувствата на луѓето за припадност кон заедница или земја - сè во обид да се подели и освои општеството на информациското бојно поле. Брзиот технолошки развој, особено во областа на вештачката интелигенција и длабоките лаги, имаат потенцијал дополнително да ја поткопаат јавната доверба во комуникациите со засилување на непријателските информациски операции, создавање конфузија во информацискатa средина и менување на перцепциите на суптилни, но значајни начини.[104]

Дезинформациите му штетат на нашето општество преку нарушување на довербата во институциите и медиумите, загрозување на изборите, отежнување на способноста на граѓаните да донесуваат информирани одлуки и ограничување на слободата на изразување. За време на кризата со COVID-19, лажните информации за вакцините, погрешните информации за здравствената заштита, опасните измами со лажни тврдења и теориите на заговор го загрозија јавното здравје. Во поново време, агресивната про-Кремљ дезинформација и воената пропаганда ја придружуваа воената агресија на Русија против Украина.[105]

За да се спротивстават на напорите на актерите кои шират дезинформации за дестабилизација на нашите општества и демократии, Кодексот на пракса за дезинформации беше објавен на 16 јуни 2022 година. 34-те потписнички, како што се платформи, технолошки компании и граѓанско општество, ги следеа упатствата на Комисијата од 2021 година и ги зедоа предвид лекциите научени од кризата со COVID-19 и руската агресивна војна во Украина. Зајакнатиот Кодекс се темели на првиот Кодекс на пракса од 2018 година, кој е широко признат како пионерска рамка на глобално ниво. Новиот Кодекс утврдува обемни и прецизни обврски од страна на платформите и индустријата за борба против дезинформациите и означува уште еден важен чекор за потранспарентна, безбедна и доверлива онлајн средина. [106]

[103] https://www.un.org/en/countering-disinformation, посетена на 21/2/2026
[104] https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats, посетена на 22/3/2026
[105] https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en, посетена на 21/2/2026
[106] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3664, посетена на 21/2/2026

Потпретседателката за вредности и транспарентност, Вера Јурова, изјави: „Овој нов Кодекс против дезинформации доаѓа во време кога Русија ги користи дезинформациите како оружје како дел од својата воена агресија против Украина, но исто така и кога гледаме напади врз демократијата пошироко. Сега имаме многу значајни обврски за намалување на влијанието на дезинформациите на интернет и многу посилни алатки за мерење на тоа како тие се спроведуваат низ цела ЕУ во сите земји и на сите нејзини јазици. Корисниците исто така ќе имаат подобри алатки за означување на дезинформациите и разбирање на она што го гледаат. Новиот Кодекс, исто така, ќе ги намали финансиските стимулации за ширење дезинформации и ќе им овозможи на истражувачите полесен пристап до податоците на платформите.“[107]

Негативното влијание од ширењето лажни вести и дезинформации може да се рефлектира на демократските капацитети на општеството, на намалување на довербата на граѓаните во демократски избраните влади, како и на перцепцијата на граѓаните дека институциите немаат капацитети да се справат со оваа негативна појава. Тие можат да предизвикаат големи штети во едно општество, без употреба на ниту еден војник и ниту едно воено средство.

Европската служба за надворешно дејствување продолжува да ја зајакнува отпорноста на мисиите и операциите на Заедничката безбедносна и одбранбена политика и и нивниот капацитет за одговор за справување со брзо развивачката закана од странско мешање и манипулирање со информации (FIMI). Во тек се дополнителни чекори за зајакнување на Системот за брзо предупредување за справување со брзо менувачката информативна средина. Работата на ЕУ со FIMI ќе биде дополнително операционализирана преку Европскиот штит за демократија, кој ќе ја зајакне способноста на ЕУ да се спротивстави на активностите на FIMI во ЕУ, а исто така ќе помогне во зајакнувањето на демократската отпорност на FIMI меѓу партнерите надвор од нејзините граници. Справувањето со FIMI во земјите-кандидатки за ЕУ ќе остане висок приоритет, особено во Украина и Молдавија, а исто така ќе ги зајакне партнерствата за борба против ваквите малигни операции во Субсахарска Африка и пошироко.[108]

Пристапот на НАТО за справување со информациските закани се потпира на тесна соработка со сојузниците и партнерите. Прво и најважно, НАТО работи со националните влади на сојузниците за справување со информациските закани. Алијансата, исто така, соработува со владите на своите партнерски земји и други меѓународни организации, како што се: Европската Унија, Механизмот за брз одговор на Г7, Обединетите нации и Организацијата за економска соработка и развој (OECD).

[107] Исто.,
[108] HR(2025) 148, https://www.parlament.gv.at/dokument/XXVIII/EU/28161/imfname_11496795.pdf, p. 50, https://www.parlament.gv.at/dokument/XXVIII/EU/28161/imfname_11496795.pdf, посетена на 21/2/2026

НАТО, исто така, се поврзува со приватни компании, медиумски организации, платформи на социјалните медиуми, организации на граѓанското општество и академски институции за да дознае повеќе за информациските закани и да развие стратегии за ублажување на нивните ефекти. Соработката со сите релевантни засегнати страни им помага на сите страни да развијат сеопфатна слика за тековните информациски закани. Секој засегнат може да се темели на сознанијата на другите, побрзо идентификувајќи ги малигните актери и непријателските наративи и реагирајќи на информациските закани на поагилен и координиран начин. Сите актери во информацискатa средина - од големи организации како НАТО до поединци во земјите-членки и партнерските земји - имаат улога во справувањето со информациските закани.[109]

3. Странското мешање и манипулирање со информации (FIMI)

Странското мешање и манипулирање со информации опфаќа широк спектар на активности, вклучително дезинформации, сајбер-напади, медиумска пропаганда и координирани влијателни кампањи, кои имаат цел да ги поткопаат демократските процеси, да предизвикаат поделби во општеството и да ги ослабат државните институции, што е сериозен предизвик за националната безбедност, јавната доверба и демократските институции.

Во многу случаи, странското мешање и манипулирање со информации (FIMI) е облик на дезинформации што јасно потекнува од извори надвор од ЕУ, но терминот опфаќа не само одредени облици на штетна содржина (дезинформации, пропаганда итн.) туку и однесувања и оперативни методи (тактики, техники и процедури), како што се напади со хакирање и протекување, компјутеризирани лажни информации и координирани автентични активности. Европскиот акциски план за демократија (2020) и Зајакнатиот кодекс на практика од 2022 година (сега Кодекс на однесување) во борбата против дезинформации споменуваат дека „странското мешање во информацискиот простор“ „честопати се спроведува како дел од поширока хибридна операција, може да се разбере како принудни и измамнички напори за нарушување на слободното основање и изразување на политичката волја на поединците од страна на странски државен чинител или негови агенти“.[110]

Странското мешање и манипулирање со информации претставува организирана, намерна и често прикриена активност на државни или недржавни актери насочена кон манипулација на информацискатa околина, заради остварување политичка, воена,

[109] https://www.nato.int/en/what-we-do/wider-activities/natos-approach-to-counter-information-threats, посетена на 22/3/2026

[110] Хаџи-Јанев М.,Стоилковски М., Странско мешање и манипулирање со информации во Република Северна Македонија, Институт за комуникациски студии, 2025, стр.14 https://respublica.edu.mk/wp-content/uploads/2025/05/stransko-meshanje-i-manipuliranje-so-informacii-vo-rsm.pdf

економска или социјална предност (EEA, 2023). Клучните карактеристики на Странското мешање и манипулирање со информации вклучуваат: (EEAS, 2025):

• манипулативен пристап – преку фабрикувани, манипулирани или селективно презентирани информации за да се создаде лажна слика за реалноста;
• ваквите активности имаат стратегиска цел – целта не е само дезинформирање, туку и влијание врз јавноста, институциите или носителите на одлуки и на тој начин да се корумпираат демократските процеси;
• примена на различни тактики и канали – употребата на Странското мешање и манипулирање со информации подразбира комбинирање на методи на класична пропаганда, дигитални манипулации, сајбер-напади, па дури и економски и дипломатски инструменти (на пример, преку повеќеслојна дипломатија или „Multitrack Diplomacy“, односно дипломатија по споредна-втора патека „Track II Diplomacy) (Diamond L., McDonald J., 1996);
• комплексни се за откривање и следење – за разлика од конвенционалната дезинформација, Странското мешање и манипулирање со информации често се спроведува на повеќе нивоа, со комплексни наративи и координирани мрежи на актери, често пати вешто затскриени помеѓу легитимните демократски процеси. [111]

Странското мешање и манипулирање со информации (FIMI) е претежно нелегален модел на однесување што се заканува или има потенцијал негативно да влијае на вредностите, процедурите и политичките процеси. Таквата активност е манипулативна по карактер, се спроведува намерно и на координиран начин. Актерите на таквата активност можат да бидат државни или недржавни актери, вклучувајќи ги и нивните застапници во и надвор од нивната сопствена територија. FIMI е сложен политички и безбедносен предизвик што претставува закана за демократските процеси и стекнувањето на сигурни информации потребни за овие процеси. Мора постојано да се анализира и разбира за ефикасно да се спротивстави.[112]

4. Градење отпорност и справување со дезинформации и странско мешање и манипулирање со информации

Инцидентите од странско мешање и манипулирање со информации (FIMI) претставуваат растечки политички и безбедносен предизвик и постои потреба од заедничка одбранбена рамка. Потребен е пристап на целото општество за да се зголеми отпорноста и да се спротивстави на странското мешање и манипулирање со информации. За да се постигне ова треба да се искористат способностите и компетенциите што лежат во владите, граѓанското општество и приватната индустрија.

[111] Исто., стр.14
[112] https://www.fimi-isac.org/index.html, посетена на 22/3/2026

На 7 февруари 2023 година, високиот претставник/потпретседател на Европската Унија, Жозеп Борел, го објави создавањето на Центар за споделување и анализа на информации на Конференцијата на EEAS за манипулација и мешање со странски информации. Центарот има за цел да го промовира споделувањето информации меѓу сите засегнати страни за основните причини, инцидентите и заканите, како и споделувањето искуства, знаења и анализи.[113]

Дополнително, истражувачкиот извештај, Стандарди за манипулација со странски информации и стандарди за одбрана од мешање: Тест за брзо усвојување на заедничкиот јазик и рамката „DISARM“ од ноември 2022 година[114], на Центарот за извонредност за борба против хибридни закани во соработка со НАТО центарот за извонредност за стратешки комуникации, придонесува за сè поголем број истражувања за одбраната од странско мешање и манипулирање со информации и се користи за да им помогне на практичарите, од различни дисциплини и сектори, да стекнат заедничко разбирање за инцидентите со странско мешање и манипулирање со информации (FIMI) и брзо да ги идентификуваат достапните контрамерки.

Се препорачува рамката DISARM да ја користат аналитичарите на закани од странско мешање и манипулирање со информации (FIMI) и практичарите за стратешки комуникации во рамките на владата, меѓународните организации и институции, платформите, академијата, приватната индустрија и граѓанското општество. Приватната индустрија треба да биде вклучена во развој на апликативен софтвер за снимање, обработка и визуелизација на информацискатa активност во согласност со рамката DISARM. Рамката DISARM е создадена како универзален пристап за идентификување и евидентирање на напади со дезинформации низ целата безбедносна заедница, како складиште со отворен извор на тактики, техники и процедури за дезинформации, како и контра-одговори на напади. Таа е креирана за да покаже како принципите и практиките за безбедност на информациите можат да се користат за зголемување на отпорноста и спротивставување на активностите за манипулација и мешање со странски информации, поточно кампањи за дезинформации.[115]

Извештајот нуди четири препораки за пошироко усвојување на рамката DISARM:

1. Рамката за DISARM треба да ја користат аналитичари на закани од странско мешање и манипулирање со информации и практичари за стратешки комуникации во рамките на

[113] https://www.fimi-isac.org/index.html, посетена на 22/3/2026
[114] Hadley N., Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework ‘DISARM’, Hybrid CoE Research Report 7, November 2022 https://www.hybridcoe.fi/wpcontent/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf, посетена на 22/3/2026
[115] https://www.disarm.foundation/framework, посетена на 22/3/2026

владата, меѓународните организации и институции, платформите, академијата, приватната индустрија и граѓанското општество.

2. Вклучување на приватната индустрија во развојот на апликативен софтвер за евидентирање, обработка и визуелизација на информацискатa активност во согласност со рамката за DISARM. Комерцијализацијата на оваа нова дисциплина и поттикнувањето на иновациите дополнително ќе ја зајакнат колективната одбрана против странско мешање и манипулирање со информации. Компаниите имаат непроценлива улога во поддршката на поширокото усвојување на DISARM преку развивање на софтверски апликации што можат да ги направат податоците употребливи и да ја откријат нивната вредност, овозможувајќи им на засегнатите страни да ја евидентираат, обработуваат и визуелизираат активноста на странското мешање и манипулирање со информации. Бидејќи онлајн практиките на странско мешање и манипулирање со информации се градат врз современи комуникациски практики, постои можност за програмерите да интегрираат компоненти на DISARM во постојните решенија за автоматизација.

3. Воспоставување на мониторинг и анализа на странско мешање и манипулирање со информации како комуникациска дисциплина во согласност со процесот на „набљудување“, „одговор“ и „анализа“ за воведување на робусни одбранбени тимови кои се применливи во владата, како и во приватната индустрија. Се предвидува дека овие организации веќе имаат поединци и тимови кои можат да се надградат за да ја задоволат растечката побарувачка за одбрана странско мешање и манипулирање со информации. Изготвувањето матрица на способности и спроведување вежба за мапирање на вештини за трите клучни дисциплини би биле почетните чекори за идентификување области за развој во рамките на организациите.

4. Подготовка на идните генерации практичари и јавноста преку соработка со академијата и професионалните тела за да се обезбеди обука соодветна на возраста. Исто како што менаџерите на социјалните медиуми и развивачите на содржини се сега мејнстрим дисциплини во областа на комуникации, специјалистите за одбрана од странско мешање и манипулирање со информации наскоро ќе го заземат своето место меѓу нив. Партнерството со професионални тела и академијата за да се предава универзален пристап би можело да ја забрза мобилизацијата на одбраната, да го зголеми базенот на таленти и да стимулира иновации во оваа нова дисциплина.[116]

[116] Hadley N., Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework ‘DISARM’, Hybrid CoE Research Report 7, November 2022, стр.51 https://www.hybridcoe.fi/wpcontent/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf , посетена на 22/3/2026,

Потребен е колективен пристап на целото општество и итна акција кои се од суштинско значење за ублажување на последиците од странското мешање и манипулирање со информации на ниво кое може да се реши само со обединет глобален одговор.

ГЛАВА IV

Анализа на напорите на Република Северна Македонија во спротивставувањето на хибридните закани и градење на капацитети и отпорност

1. Хибридни закани и градење национална отпорност

Република Северна Македонија е изложена на синхронизирани и координирани хибридни активности на државни и недржавни субјекти (невладини организации, партиски лица, верски и други структури, јавни личности, маргинални групи). Преку широк опсег на мерки од овие актери, кои вклучуваат: политичка субверзивност; економски притисок; сајбер активности; финансирање на медиуми (пропаганда и ширење на дезинформации); злоупотреба на интернет портали; платформи и социјални мрежи; инвестирање во сектори, кои се клучен национален интерес, особено во енергетиката се обидуваат да ја попречат соработката со ЕУ и НАТО, да ја блокираат европската интеграција на земјата и евроатлантската интеграција на регионот, да ги зголемат социјалните поделби и да негуваат етнички национализам, да предизвикаат вознемиреност кај граѓаните и да ја поткопаат довербата во институциите на системот.[117]

Градењето отпорност од хибридни закани е обврска на целото општество. Сите државни институции имаат улога, обврски и задачи во справувањето со овие закани, во рамките на своите надлежности. Дополнително, истите се упатени кон соработка со приватниот и граѓанскиот сектор. Клучен институционален субјект за функционирање на државата во случај на справување со хибридни закани е Владата, која ќе се подготви за континуирано и координирано делување, во состојба кога земјата ќе се соочи со хибридни закани.[118]

Република Северна Македонија работи на справување со хибридни закани и поврзаните ризици преку сеопфатен меѓуинституционален и владин пристап и соработка, вклучувајќи ги сите нивоа на државата и општеството. Надградбата и изградбата на отпорни системи на државата и општеството се клучни за рано откривање, брз одговор и одбрана од различни форми на хибридно влијание.

Република Северна Македонија се приклучи на Европскиот центар за извонредност за справување со хибридни закани, со седиште во Хелсинки на 27.10.2023 год, со што се отвори можност за зајакнување на националните капацитети за справување со овој вид предизвици. Со вмрежувањето во Центарот се создаде можност за размена на информации, искуства и најдобри практики, преку учеството на наши експерти во Центарот и користење на експертиза од истиот. Секоја година Центарот

[117] Национална стратегија за безбедност на Република Северна Македонија 2024-2029, стр.12
[118] Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.25

спроведува билатерални консултации со земјите членки, вклучително и со Северна Македонија, во насока на ефикасна соработка во справувањето со хибридните закани.

Во насока на унапредување на соработката со ЕУ, на 19 ноември 2024 беше потпишано Партнерството за безбедност и одбрана помеѓу Европската Унија и Република Северна Македонија за воспоставување и имплементирање заемно корисно партнерство кое ќе ја обликува соработката во безбедносниот и одбранбениот спектар помеѓу ЕУ и Република Северна Македонија. Како посебни тематски области се вклучени: хибридните закани и сајбер безбедноста, како и зајакнување на комуникацијата во правец на заштита од влијание на странски манипулативни информации, иницирање на тренинг и обука итн. Првиот дијалог во рамките на партнерството се одржа во Скопје во мај 2025 година, а вториот дијалог е планиран на крајот на април во Брисел, каде една од темите ќе биде посветена на справувањето со хибридните закани.

2. Стратегија за градење отпорност и справување со хибридни закани 2021-2025

На Стратегијата за градење отпорност и справување со хибридни закани 2021-2025 и претходеше истражување на ранливоста на Република Северна Македонија од хибридни закани, изработено во соработка со Европската служба за надворешно дејствување (EEAS), во 2019 година, а во согласност со Заедничката рамка на ЕУ за справување со хибридни закани од 2016 година. Меѓуресорската работна група која работеше на изработката на одговорите на индивидуализираниот Прашалник за хибридни закани за Република Северна Македонија беше составена од соодветни претставници од 28 институции, координана од Министерството за одбрана. Во согласност со одговорите на прашалникот, ЕУ идентификуваше клучни области на ранливост од хибридни закани и формулираше препораки за зајакнување на отпорноста на Северна Македонија против хибридни закани кои Владата ги прифати на 47-та седница, на 28.04.2020 година. Следен чекор беше изработката на Стратегија и Акциски план за градење отпорност и справување со хибридни закани 2021-2025 кои беа одобрени од страна на Владата на 5 октомври 2021 година.

Целта на стратегијата е создавање заедничка свест за природата на хибридните закани, мапирање на обврските и носителите, идентификување на начините за делување, како и креирање ресурси за градење национална отпорност со ангажирање на целокупното општество, што подразбира и изградба на општество подготвено за рана детекција, за одговор и брзо заздравување, со учество на сите релевантни чинители во справувањето со хибридните закани.[119]

[119] Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.14-18

Активностите на државата се поделени во шест области на оперативни активности.

Оперативни области

Слика бр.2. Извор: Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.13

Цели во шесте оперативни области:

- **Првата област** на оперативни активности е во сферата на политиката. Клучен ефект кој треба да се постигне во оваа област е континуитет на власта. За таа цел ќе се изгради систем за рано предупредување и известување за евентуални закани, како и идентифукување и подготовка на клучниот персонал. Исто така, ќе се обезбеди ефикасен систем за управување со кризи во поддршка на владините активности во време на криза, со резервни капацитети за независно функционирање за период од еден месец, како и безбедни комуникациски врски.

- Воедно, во рамките на оваа област ќе се обезбеди заштита и на изборниот процес од хибридни закани, непријателски сајбер-активности, информативни операции спроведувани од други државни и недржавни субјекти и финансирање на политички партии, политичари и невладини организации од страна на надворешни, непријателски фактори. За ефикасно постигнување на оваа цел, националните носители ќе ги користат научените лекции и експертиза од НАТО и ЕУ.
- **Втора област** на оперативни активности е развојот на економијата и поволна бизнис клима. Ефектот кој треба да се постигне во оваа област е воспоставување функционален механизам за справување со ризици поврзани со странски директни инвестиции. Создавањето услови за развој на домашното стопанство дополнително треба да постигне значајна трговска и енергетска независност. Креирањето услови за дигитална економија ќе овозможи конкурентност на домашните компании на пазарите во светот, особено на ЕУ пазарот, како и отворање нови работни места и нивна брза трансформација на промените на пазарот. Суштинска активност во оваа област е борбата против корупцијата.
- **Трета област** на оперативни активности се воените и безбедносни сили и институции т.е. одбранбено-безбедносниот сектор. Во оваа област клучно е креирањето способност на воено-безбедносните сили и на капацитетите за управување и поддршка во услови на кризи, со цел зголемување на отпорноста на општеството за справување со хибридни закани. Фактот дека при хибридна закана е минимизирана употребата на конвенционалните вооружени сили, упатува на потребата од континуирано унапредување на одбранбено-безбедносните механизми. Во таа насока потребно е да се постигне висока способност за справување со повеќе истовремени напади врз цивилни и воени цели, способност за воспоставување ефикасен механизам за безбедност на ресурсите со храна и вода, справување со неконтролирано движење на значителен број луѓе и справување со инциденти кои резултирале со голем број жртви. Дополнително, разузнавачките субјекти на Република Северна Македонија треба да одржуваат континуирана меѓусебна соработка и соработка со разузнавачките институции на ЕУ и НАТО, одговорни за процена на хибридните закани.
- Безбедноста при хибридни закани ја опфаќа и безбедноста на јавното здравје, кое може да биде загрозено преку преносливи болести или преку контаминација на храна, почва, воздух и вода со хемиски, биолошки, радиолошки и нуклеарни агенси. Намерното ширење на епидемиолошки заболувања може значително да ја загрози безбедноста на храната и да има далекосежни неповолни економски ефекти. За справување со вакви закани, членките на ЕУ се поврзани преку Систем

за рано предупредување и одговор [120]. Дополнително, во областа на безбедноста на храна, членките на ЕУ разменуваат информации и анализи преку Итниот систем за предупредување за храна и храна на животните[121] и Заедничкиот систем за менаџмент на ризик за царини[122] . Следствено, Република Северна Македонија ќе развива национални способности за заштита на јавното здравје од хибридни закани и ќе воспостави ефективна соработка со институциите на ЕУ во оваа област.

- **Четврта област** на оперативни активности е граѓанското општество. Всушност, хибридната војна е дизајнирана за постигнување општествени поделби и предизвикување немири за соборување на власта, пред сè, преку дезинформативни и психолошки операции. Затоа, потребно е создавање на способност за критичка свест и медиумска писменост кај граѓаните на Република Северна Македонија. Друга состојба која треба да се постигне во граѓанскиот сектор е постигнување високо ниво на меѓуетничка и меѓуверска толеранција.
- **Петта област** на оперативни активности е информативниот сектор. Клучен ефект потребен за справување со хибридни закани во овој сектор е создавање способност за детекција на дезинформативни и психолошки операции, како и способност за справување со интернет „тролови" и користење вештачка интелигенција во процесот на ширење лажни вести и дезинформации. Еден од ефектите кој треба да се постигне е создавање постојан и ефективен систем за стратегиска комуникација, директно воден од Владата на Република Северна Македонија, а во соработка со други релевантни државни институции. Дополнително, треба да се постигне состојба во која јавниот радиодифузен сервис ќе спроведува плански активности за справување со лажните вести и дезинформации. Воедно, државата ќе ги поддржува здруженијата на граѓани кои се активни во справувањето со дезинформации.
- **Шеста област** на оперативни активности е заштитата на критична инфраструктура на Република Северна Македонија. Прв ефект кој треба да се постигне е донесување законско решение со кое ќе се детерминира критичната инфраструктура, како и донесување регулативи за нејзина заштита. Во овој контекст, регулативите на ЕУ и НАТО ќе бидат рамка за идните активности на Република Северна Македонија во детерминирањето и обезбедувањето на критичната инфраструктура.[123]

Друг суштински елемент за справување со хибридните закани, поврзан со критичната инфраструктура, е диверзификацијата на изворите на енергија и

[120] Early Warning and Response System
[121] Rapid Alert System for Food and Feed
[122] Common Risk Management System for Customs
[123] Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.14-18

снабдувачите. За ова да се постигне потребно е поседување инфраструктура која ќе овозможи високо ниво на енергетска независност на Република Северна Македонија од индивидуални надворешни снабдувачи на енергија. Истиот концепт на избегнување зависност треба да се користи и во однос на инфраструктурата заснована на нови технологии како мобилната, интернет и сателитската комуникација. Република Северна Македонија, во однос на одредувањето на критичната инфраструктура и планирањето на нејзината безбедност, ќе го има предвид технолошкиот развој и влијанието на нови високи технологии.

Република Северна Македонија треба да создаде безбедна сообраќајна инфраструктура, сигурни енергетски извори и транспорт, телекомуникациска мрежа, стабилен здравствен и социјален систем, независни медиуми и економско-финансиски систем, како базичен дел од критичната инфраструктура, бидејќи комплексноста на хибридните закани бара целосна вклученост на сите институционални чинители во системот на национална безбедност.

3. Организациска структура во Република Северна Македонија за спроведување на Политиката на НАТО за градење отпорност

НАТО ги поддржува сојузничките нации во процесот на проценка и подобрување на нивната цивилна подготвеност. Во 2016 година, на Самитот во Варшава, сојузничките лидери се обврзаа да ја зголемат отпорноста преку стремеж кон постигнување на седум основни барања за цивилна подготвеност:

1. Обезбеден континуитет на владата и критичните владини услуги;

2. Отпорни резерви на енергија;

3. Способност за ефикасно справување со неконтролирано движење на луѓе;

4. Отпорни ресурси за храна и вода;

5. Способност за справување со масовни жртви;

6.Отпорни системи за цивилна комуникација;

7. Отпорни системи за цивилен транспорт.

Оваа обврска се заснова на признавањето дека стратешката средина се променила и дека отпорноста на цивилните структури, ресурси и услуги е првата линија на одбрана за денешните модерни општества.

Како членка на НАТО, Република Северна Македонија има обврска да ја зголеми националната отпорност кон целиот спектар закани и да ги имплементира т.н. седум основни потреби/побарувања за национална отпорност. Овие потреби се поставени за поддршка на трите основни функции на цивилната подготвеност: континуитет на владата, континуитет на основните услуги за населението и цивилна поддршка на армијата. Покрај обврската за колективна одбрана, Република Северна Македонија, како НАТО членка, има обврска да гради и да одржува адекватна цивилна подготвеност и отпорност. Градењето отпорност е во согласност со членот 3 од Северноатлантскиот договор, односно со обврската за колективно и индивидуално развивање на капацитети за одговор на каква било форма на закана или криза.[124]

Во согласност со заклучок од Записникот на Седумдесет и втората седница на Владата на РСМ одржана на 23.08.2022 година, Центарот за управување со кризи е надлежна институција за координација на спроведување на политика на НАТО за градење отпорност. Во согласност со горенаведениот заклучок Центарот беше задолжен во рок од 60 дена да формира Координативно тело за спроведување на политика на НАТО за градење отпорност.

Со одлуките на Владата од јули и август 2022 година формирано е Национално координативно тело (Меѓуагенциска работна група) за спроведување на Политиката на НАТО за градење отпорност. Национален координатор (водечка организација) е Центарот за управување со кризи[125], а учествуваат 30 институции-членки - владини институции и јавни претпријатија. Предвидени се 7 водечки институции: Генерален секретаријат на Владата и следните министерства: Министерство за енергетика, рударство и суровини; Министерство за внатрешни работи; Министерство за земјоделство, шумарство и водостопанство; Министерство за здравство; Министерство за дигитална трансформација; Министерство за транспорт.

Во согласност со основните барања на НАТО тие се поделени во седум подгрупи [126]:

1. Обезбеден континуитет на владата и критичните владини услуги

Институција носител: Генерален секретаријат на Владата

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за транспорт, Министерство за земјоделство, шумарство и водостопанство, Министерство

[124] Стратегија за градење отпорност и справување со хибридни закани, април 2021, стр.6
[125] Согласно заклучок од Записникот на Седумдесет и втората седница на Владата на РСМ одржана на 23.08.2022 година, Центарот за управување со кризи е надлежна институција за координација на спроведување на политика на НАТО за градење отпорност. Согласно горенаведениот заклучок Центарот беше задолжен во рок од 60 дена да формира Координативно тело за спроведување на политика на НАТО за градење отпорност.
[126] НАТО документ: PO(2023)0226 – 2023 Alliance Resilience Objectives

за животна средина и просторно планирање, Министерство за здравство, Министерство за внатрешни работи, Министерство за надворешни работи и надворешна трговија, Министерство за економија и труд, Министерство за локална самоуправа, Министерство за дигитална трансформација, Министерство за социјална политика, демографија и млади, Министерство за енергетика, рударство и суровини, Министерство за јавна администрација, Министерство за финансии - Царинска управа, Центарот за управување со кризи, Дирекција за заштита и спасување, Агенција за национална безбедност.

Цел: Воспоставување ефикасен систем за рано предупредување, известување и алармирање како дел од нивното планирање за пандемија со јавни и приватни засегнати страни за да помогнат во превенцијата и раното предупредување, и да обезбедат безбедни основни комуникации кога примарните работни локации не се употребливи (алтернативни локации/работа од далечина итн.)

Владата поддржана од Центарот за управување со кризи ќе развие формализиран план за континуитет на Владата, вклучувајќи и нивоа на раководење и јасност на процесот на донесување одлуки и синџир на командување во Владата во случај на катастрофален настан. Ова ќе вклучува идентификација и приоритизирање на клучните владини агенции, критичните услуги и задолжителните функции за поддршка на воените операции, вклучително и функциите како што се обезбедување и испорака на храна, вода, гориво, електрична енергија, топлина, транспорт, специјализирани стоки и медицински/фармацевтски производи и опрема за лична заштита. [127]

2. Отпорни енергетски резерви

Институција носител: Министерство за енергетика, рударство и суровини

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за транспорт, Министерство за внатрешни работи, Министерство за надворешни работи и надворешна трговија, Министерство за економија и труд, Министерство за дигитална трансформација, МЕПСО - Македонски оператор на електроенергетскиот систем, ЕВН - компанија за дистрибуција на електрична енергија, ЕСМ - Електрани на Северна Македонија.

Министерство за енергетика, рударство и суровини ќе развие планови и ресурси за да обезбеди непрекинат пристап до сигурна енергија, особено во време на криза, имајќи го предвид потенцијалното влијание на меѓузависноста, каскадните ефекти и потенцијалните второстепени влијанија. Во случај на прекин, достапноста на сеопфатни,

[127] Национална стратегија за безбедност на Република Северна Македонија 2024-2029, стр.22

одржливи и вишок способности и сигурни планови за обнова ќе резултираат со намалени прекини и намалено време за обнова на услугата.

Цел: фокус на континуираниот пристап до сигурни енергетски резерви во време на криза, потенцијалното влијание на новите и напредни технологии, диверзификацијата на снабдувањето со енергија и аранжманите за следење и проценка на странските директни инвестиции, сопственоста и оперативната контрола на критичните системи и инфраструктура.

3. Способност за ефикасно справување со неконтролирано движење на луѓе

Институција носител: Министерство за внатрешни работи

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за транспорт, Министерство за здравство, Министерство за надворешни работи и надворешна трговија, Министерство за социјална политика, демографија и млади, Министерство за финансии - Царинска управа, Дирекција за заштита и спасување, Агенција за национална безбедност.

Цел: се фокусира на одредби што го ограничуваат движењето на луѓето во исклучителни околности, како што е очигледна опасност од губење на живот поради природни катастрофи; епидемии што го загрозуваат животот, пандемии или хемиски, биолошки, радиолошки и нуклеарни (ХБРН) закани; или за поддршка на барањата на НАТО или националните воени потреби.

Министерството за внатрешни работи, врз основа на законски пропишани протоколи, ќе развие интегриран национален план за решавање и справување со влијанието од неконтролирано движење на луѓе внатре, но и надвор од националната територија, вклучително и голем прилив на луѓе што надминува 2% од вкупното население. Целта на ваквиот план е да се предвидат механизми преку кои ќе се осигури заштита на населението во случај на животозагрозувачки опасности, имајќи ги предвид основните човекови потреби (здравје, вода, санитарни услови и хигиена, храна, засолниште, безбедност и транспорт).[128]

4. Отпорни ресурси за храна и вода

Институција носител: Министерство за земјоделство, шумарство и водостопанство

[128] Исто, стр.21

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за транспорт, Министерство за внатрешни работи, Министерство за економија и труд, Министерство за животна средина и просторно планирање, ЈП „Водовод и канализација“ – Скопје, Агенција за храна и ветеринарство, Агенција за стоковни резерви, Агенција за национална безбедност.

Цел: Развој на сеопфатен план за континуитет за решавање на ограничената достапност на основните елементи на работната сила, способности на експертите, суровините, критичните залихи, меѓусекторските разгледувања како и други ресурси потребни за обезбедување континуирано снабдување со храна и вода.

Министерство за земјоделство, шумарство и водостопанство ќе развие сигурен систем за надзор, детекција, тестирање и пријавување на загадување на изворите на храна и вода и клучната инфраструктура. Понатаму, ќе спроведе сеопфатно планирање за вонредни состојби, редовни вежби и обезбедување на алтернативни извори за снабдување со храна и вода и сеопфатно планирање на континуитетот за идентификување на суштинските функции и можните начини за тие да се одржуваат.[129]

5. Способност за справување со масовни жртви

Институција носител: Министерство за здравство

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за транспорт, Министерство за надворешни работи и надворешна трговија, Министерство за внатрешни работи, Министерство за економија и труд, Агенција за стокови резерви, Дирекција за заштита и спасување, Агенција за национална безбедност.

Цел: Фокус на подобрување на робусноста на аранжманите за национална безбедност на снабдувањето со медицински контрамерки, земајќи ги предвид постојните и потенцијалните ранливости во релевантните синџири на снабдување; мерки за обезбедување и заштита на здравствените установи/системи и одредена опрема за здравствена заштита; и идентификација на критични здравствени работници потребни за поддршка на основните функции во случај на сериозно нарушување на достапноста на работната сила, како на пример за време на епидемија/пандемија. Исто така, се справува со сајбер ризиците за здравствените системи и синџирот на снабдување со медицински средства.

Министерството за здравство ќе развие планови и политики за да изгради подготвеност и планирање за соочување со појава на масовни жртви и здравствени кризи

[129] Исто,.стр.26

(кадровски и итен капацитет, капацитет за транспорт на пациенти, сеопфатна инфраструктура и кризни комуникации). [130]

6. Отпорни цивилни комуникациски системи

Институција носител: Министерство за дигитална трансформација

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за надворешни работи и надворешна трговија, Министерство за внатрешни работи, Агенција за електронски комуникации

Цел: разгледување на последиците од странска сопственост/контрола/директни инвестиции; потенцијалните ранливости поврзани со новите и напредни технологии, како што е 5G; како и воспоставување робусни протоколи/постапки за безбедност на информациите што ја опфаќаат сајбер безбедноста. Ова ажурирање им советува на земјите да вклучат мерки за планирање во случај на пандемија во нивните планови за непредвидени ситуации за инфраструктурата на информатичката технологија (ИТ), на пример за управување со зголемениот обем на интернет сообраќај.

Министерството за дигитална трансформација ќе развие планови и политики за да обезбеди непрекината достапност и пристап до сигурни, безбедни и сеопфатни комуникациски услуги во мирно време, во криза, кризна состојба, во вонредна и во воена состојба, имајќи ги предвид потенцијалните ризици (сајбер, физички, кадровски, хибридни, предизвикани од човечки фактор или природни катастрофи, пандемии, епидемии, климатски промени, последици од странско сопственишство, контрола или директни инвестиции), како и оние потенцијални ранливости поврзани со постојните и новите технологии, како што е 5Г.[131]

7. Отпорни системи за цивилен транспорт

Институција носител: Министерство за транспорт

Учествуваат во поддршка: Министерство за одбрана/Армија, Министерство за внатрешни работи, Министерство за надворешни работи и надворешна трговија, Министерство за економија и труд, Министерство за дигитална трансформација, Министерство за енергетика, рударство и суровини, Министерство за финансии - Царинска управа, Агенција за национална безбедност, M-NAV - Македонски давател на услуги за воздухопловна навигација, Агенција за цивилно воздухопловство, ЈП Одржување и заштита на јавни и регионални патишта - Скопје, ЈП Железничка

[130] Национална стратегија за безбедност на Република Северна Македонија 2024-2029, стр.21
[131] Исто., стр.27

инфраструктура - Железници на Северна Македонија - Скопје, ЈП „Водовод и канализација“ - Скопје, Агенција за електронски комуникации, ТАВ Македонија - Меѓународен аеродром Скопје.

Цел: Фокус на важноста на воспоставување аранжмани за обезбедување достапност на средства за цивилен/комерцијален транспорт, инфраструктура, услуги и транспортни правци за поддршка на националните приоритети за време на кризи и за обезбедување обновување на овие транспортни капацитети по кризи; да се воспостават законски одредби за реквизиција, користење или располагање со национални/странски транспортни ресурси; да се обезбеди одржлива и отпорна мрежа на синџирот на снабдување; и да се обезбеди дека земјите имаат можност да создаваат посебни транспортни коридори за приоритетни воени и цивилни возила и товар.

Министерството за транспорт и врски ќе развие политики и механизми за да се осигури дека: инфраструктурата за цивилен транспорт е отпорна, агилна, сеопфатна и способна да се спротивстави и да закрепне со мали прекини од влијанието на различни потенцијални ризици (пр. природни несреќи или несреќи предизвикани од човечки фактор, хибридни закани, сајбернапади, пандемија, климатски промени); последиците на странско сопственишство, контрола или директни инвестиции, како и оние потенцијални ранливости поврзани со постојните и новите технологии, како што се 5Г и потенцијалните ранливости се поврзани со продолжени кризи.[132]

Улогата на МО/Армијата во градењето отпорност

Министерството за одбрана/Армијата (како витални државни субјекти со значајни капацитети/способности) во процесот на спроведување на Политиката на НАТО за градење отпорност имаат значајна улога во поддршката на институциите одговорни за градење на одредени линии на отпорност.

Задачи на Армијата во поддршка на институциите: поддршка на цивилните власти во справувањето со природни катастрофи и ублажување на последиците; поддршка на цивилните власти во случај на големи болести и епидемии; поддршка на цивилните власти во случај на технички/технолошки катастрофи; поддршка на цивилните власти во случај на деградација и уништување на животната средина; поддршка на полицијата против безбедносни закани, ризици и опасности во случај да не се во можност да се справат со сопствените капацитети.

[132] Исто.,

Обуки и вежби за отпорност (организирани од МО)

Преку серија настани (работилници и вежби) планирани со SSCI (Significant Security Coordination Initiative) во рамките на билатералната соработка помеѓу САД (Institute for Security Governance – ISG/ Институт за безбедносно раководење) и Министерството за одбрана на Северна Македонија, до 2027 година, Северна Македонија, како млада членка на НАТО, ќе може да постигне избрани цели утврдени во рамките на седумте основни барања за отпорност на НАТО (вклучени во Процесот на планирање на одбраната на НАТО), кои ја поддржуваат интероперабилноста со Системот за одговор на кризи на НАТО; Национална политика, пракса и способности за отпорност што одразуваат пристап на целата влада, ги опфаќаат барањата за поддршка на земјата домаќин и се потврдени преку домашни, регионални, вежби на USEUCOM[133] и НАТО. Целна група за обука се членовите/заменици-членови на Националното координативно тело (Меѓуагенциска работна група) за градење отпорност.

Во 2023 и 2024 година во рамки на билатералната соработка помеѓу Министерството за одбрана на Република Северна Македонија и Соединетите Американски Држави се реализираа четири Меѓуресорски работилници за градење отпорност во организација на Министерството за одбрана и Институтот за безбедносно раководење (Institute for Security Governance - ISG) од САД. Работилниците се водени од тим на експерти од САД, кои се вклучени во процесот на одбранбено планирање на НАТО. Учесниците на работилниците се воедно и членови во Координативното тело за спроведување политика на НАТО за градење отпорност. Претставниците на ЦУК учествуваа во својство на координатори и коносители во сите 7 линии на градење отпорност.[134]

Во тој контекст, од 25 до 27 март 2025 година во Скопје, во ко-организација на Министерството за одбрана и Американскиот институт за безбедносно управување се реализираше работилница за градење на отпорност помеѓу институциите во државата.[135] Целта на работилницата беше унапредување на знаењата за напредно планирање на процесот за имплементација на основните барања на НАТО за отпорност и развој на концепциско-плански документи поврзани со обезбедување на континуитет на владата, справување со масовни жртви, поддршка на земја-домаќин, како и поддршка на меѓу-агенциската/цивилно-воената соработка поврзана со отпорноста, управувањето со кризи и подготвеноста за одговор на сите опасности. На работилницата учествуваат

[133] Европската команда на САД (USEUCOM) е една од 11-те Обединети борбени команди во американската војска и нејзина примарна одговорност е да обезбеди команда и контрола на американските воени сили во Европа за заштита и одбрана на САД и нивните сојузници и партнери од НАТО преку одвраќање, мировни операции и воени операции.
[134] Нацрт стратешки план на Центарот за управување со кризи за период 2025-2027 год., од август 2024
[135] https://mod.gov.mk/mk-MK/medija-centar/informacii-od-ministerstvoto/zapocna-rabotilnicata-za-gradenje-na-otpornost-vo-makedonskite-institucii, посетена на 15/4/2026

претставници од министерства и други институции поврзани со одбраната, безбедноста, здравството, транспортот, енергетиката и комуникациите одговорни во градење на отпорноста на општеството.Оваа работилница е континуитет на НАТО работилниците за градење на отпорност реализирани во текот на 2023 и 2024 година. Дополнително, во декември 2025 година се одржа работилница за градење отпорност на национално ниво[136], реализирана во соработка со Институтот на САД за безбедносно управување, во рамките на која се реализираше вежба која ја тестира националната подготвеност за колективна одбрана и отпорност и овозможи вмрежување помеѓу професионалците од над триесет институции и оператори на критичната инфраструктура. Овие активности овозможуваат зајакнување на меѓуинституционалната координација и утврдување на следните чекори, со цел поефикасен и отпорен систем во служба на граѓаните.

Република Северна Македонија со свои претставници учествува на состаноците на Комитетот за градење отпорност во седиштето на НАТО во Брисел.

Во текот на 2023 година упатено е лице од Центарот за управување со кризи во Постојана делгација на Република Северна Македонија при НАТО во Брисел со цел активно учество во работата на НАТО комитетите и работните групи и поефикасна комуникација, координација и размена на иформации од областа на Цивилната подготвеност.[137]

Комплексната безбедносна конталација денес, бара од сојузниците засилен ангажман во делот на исполнување на обврските преземени со последните одлуки донесени на Самитот на НАТО во Хаг.

Инвестиции поврзани со одбраната и безбедноста (1,5% од БДП) за градење отпорност и справување со хибридни закани

На самитот во Хаг 2025 сојузниците на НАТО се обврзаа да ги зголемат своите трошоци за одбрана од сегашната цел од 2% од БДП на 5% до 2035 година. Од овој вкупен износ, 3,5% (одбранбени трошоци) треба да бидат наменети за „основна“ одбрана, додека 1,5% ќе бидат наменети за „помеки“ приоритети како што се зајакнување на цивилната инфраструктура и поттикнување на иновациите.

[136] https://mod.gov.mk/mk-MK/medija-centar/novosti/rabotilnica-za-gradenje-na-otpornost-pomegju-nacionalnite-institucii, посетена на 15/4/2026
[137] Нацрт стратешки план на Центарот за управување со кризи за период 2025-2027 год.,август 2024, стр.20

Дефиниција: [138]

Под инвестиции поврзани со одбраната и безбедноста (1,5% од БДП) се подразбираат трошоците направени на сите ниво на власта во поддршка на трите клучни задачи на Алијансата (одвраќање и одбрана, превенција и менаџирање на кризи и кооперативна безбедност), а кои не се во рамките на првата категорија на трошоци – Одбранбени трошоци (3,5%).

Во согласност со дефиницијата, подолу се вклучени сите активности во поддршка на НАТО и националните планови, развој на индустриски капацитети и иновации, зајакнување на отпорноста и цивилната подготвеност, поддршка на партнерите и справување со хибридни закани (напади, операции и дестабилизирачки кампањи): [139]

Категории на инвестиции:[140]

Цивилни активности и способности (трошоци за цивилно-воени и цивилни активности, капацитети и услуги кои не се опфатени со Одбранбените трошоци (3,5%), а се во поддршка на НАТО плановите или на националните планови (воени и за отпорност). Како примери се наведени: трошоци на институциите за сајбер безбедност или агенции (пр. Computer Emergency Response Teams), разузнавачки агенции (надвор од одбраната), активности поврзани со гранична безбедност и справување со нелегална миграција, активности за борба против тероризам, контактирани услуги кои треба да обезбедат услуги во услови на криза и војна, трошоци за опрема и оперативни трошоци на силите (не-воени) кои е планирано да се ангажираат во поддршка на НАТО плановите или на националните планови (воени и за отпорност).

Отпорност и цивилна подготвеност (трошоци за отпорноста, цивилната одбрана и цивилна подготвеност кои се базирани на националното планирање за отпорност или се неопходни во поддршка на НАТО плановите). Како примери се наведени:[141] трошоци за имплементација на националните цели за отпорност (обезбедување критични владини услуги, одржливо обезбедување на енергија, справување со неконтролирано движење на луѓе, безбедност на храна и вода, справување со ситуации на масовни жртви, сигурни комуникации, обезбедување сигурен транспорт/инфраструктура - сигурност на линиите на снабдување на добра и услуги), трошоците за воспоставување на поддршка од земја домаќин (HNS), трошоците за обука и вежби наменети за тестирање на механизмите за имплементација на

[138] НАТО документ AC/281-WP(2025)0043-REV7 (R) -The Defence and security related Investments definition
[139] НАТО документ PO(2025)0158) – Revised Strategy on NATO's role in countering hybrid actions
[140] Набројувањата подолу се дел од НАТО документот AC/281-WP(2025)0043-REV6 (R), ANNEX 1
[141] НАТО документи:PO(2022)0037 – Establishing Resilience Objectives and nationally-developed goals; PO(2023)0226 – 2023 Alliance Resilience Objectives; PO(2024)0243 – Delivering stronger resilience for the Alliance; PO(2024)0322 – Roadmap for the development of non-binding guidance to support national civilian planning; PO(2025)0144 – Non-binding guidance to support national civilian planning

националните Цели за отпорност, активности за заштита од употреба на политички, економски, енергетски, информациски и други хибридни тактики од државни и недржавни актери.

Капацитети на одбранбена индустрија (проширување, пренамена, унапредување на воената индустрија (инвестиции во директна поддршка на производството) /Национални, здружени, мултинационални инвестиции во одбранбено или производство поврзано со одбраната. Како примери наведени се: капацитети за производство на воено-медицинска опрема, инвестиции во човечки капитал во оваа област, финансиска поддршка на државни или приватни одбранбени или поврзани со одбраната компании.

Иновации (инвестиции во проширување на иновацискиот одбранбен екосистем и поттикнување на раст на добавувачи на воени средства и средства со двојна намена). Како примери наведени се: инвестиции во strat-ups, технолошки компании, академската заедница, технолошки институти во насока на развој, иновации, истражување за воени и безбедносни цели.

Складирање (трошоци за складирање на резерви потребни за одржување на производството на опрема за одбрана и безбедност/**т**рошоци за складирање на опрема и средства за потребите на планирањето на отпорноста на државата).

Инфраструктура (трошоци за изградба, проширување, замена и одржување на инфраструктура наменета за поддршка на НАТО плановите или на националните планови (воени и за отпорност)/трошоци за заштита и физичка безбедност на критичната инфраструктура, трошоци за обезбедување пристап кон критичната инфраструктура. Како примери наведени се: мостови, железница, тунели, аеродроми и патна инфраструктура што побарува поголеми класификации за воен товар.

Воена и финансиска програма за помош и финансиски контрибуции (воена и финансиска помош на НАТО партнерите во поддршка на нивните воени и безбедносни напори/финансиска контрибуција на партнерска организација во поддршка на воените и безбедносните напори на партнерите или земјите членки на НАТО. Како примери наведени се: финансиска контрибуција во ООН, ЕУ, ОБСЕ (средства кои се користат за помош на одделни земји и кои можат да се прикажат), други облици на донации на партнери од страна на другите безбедносни институции.

4. Напори за заштита и отпорност на критичната инфраструктура

Прашањето на критичната инфраструктура е дел од еден покрупен мозаик кој претставува предизвик во изградбата на висок степен на отпорност на нашето општество

и неопходно е да се подигне свесноста и нивото на подготвеност за заштита на критичната инфраструктура во рамки на стратешкото управување со државата и нејзините институции, вклучително и изградба на интегрирана легислативна рамка за заштита на критичната инфраструктура. Потребно е да се изгради вмрежен систем и заштита на критичната инфраструктура, кој не може да биде едносекторски и парцијален туку насочен кон рано предупредување и превенција.[142]

Критичната инфрастурктура е од витално знчаење за фунционирањето на една држава, а доколку дојде до нејзино оштетување, унишутување или загуба доведува до губење на испоракта на услугите кои зависат од нејзино непречено функционирање. Критичната инфраструктура поимно би можеле да ја определиме како инфраструктура што е суштествено, животно неопходна, а нарушувањето на нејзиното нормално функционирање може да доведе до загрозување на најзначајните вредности и добра врз коишто почива државата, општеството, економијата, благосостојбата и воспоставениот начин на живот. Од таму произлегува дека, критичната инфраструктура се системи, мрежи и објекти кои пружаат основни услуги во едно општество, па претставуваат поддршка за успешено функционирање на стопанството, сигурност и заштита на здравјето и благосостојбата во државата. Сигурноста и заштитата на здравјтето и благосостојбата во државата зависи од сигурноста и отпорноста на критичната инфраструктура. [143]

Планирањето, организирањето и спроведувањето на заштитата на критичната инфраструктура и обезбедувањето на максимален степен на безбедност е клучен приоритет. Денеска сме соочени со широк спектар на закани и безбедносни предизвици од различна природа со различен степен на интензитет и различни носители кои директно или индиректно ја загрозуваат критичната инфраструктура во Република Северна Македонија.

Имајќи во предвид дека критичната инфраструктура претставува платформа за одржување на развојот на секое општество и држава, Владата треба да биде вклучена во системот на заштита на критичната инфраструктура како предлагач на закони и подзаконски акти и има задача да им даде овластување на одредени министерства да бидат координатори на целиот систем. Владата обезбедува стратегиска рамка која е од суштинско значење за успешно функционирање на системот, соработката, комуникацијата и координацијата на сите вклучени актери. Владата, исто така ги одредува (со посебна одлука) секторите од одредени критични инфраструктури со цел

[142]https://arhiva.mod.gov.mk https://arhiva.mod.gov.mk arhiva.mod.gov.mk/петровска-од-конференцијата-за-крити/посетена на 15/4/2026

[143] Предлог на Закон за критична инфраструктура, 2022, достапен на https://portal.mdt.gov.mk/post-body-files/legislativa-mod-file-iCuk.pdf

да обезбедат холистички пристап за заштита и намалување на негативните влијанија во случај на закана за критичната инфраструктура.

Со Предлог на Законот за критична инфраструктура[144] ќе се дефинира националната инфраструктура како инфраструктура од суштинско значење за одржување на виталните општествени функции, здравјето, безбедноста, сигурноста, економската или социјалната благосостојба на луѓето и животната средина и градењето на отпорноста на субјектите на критичната инфраструктура. Со Законот ќе се изврши усогласување со Директивата на Европската унија 2008/114/ЕК, за одредување и иднентификација на европските критични инфраструктури и процена за потреба од унапредување на нивната заштита (СЛ Л 345/75, 23.12.2008) како и Директивата на Европскиот парламент и Советот на ЕУ 2022/2557/ЕК од 14 декември 2022 година за отпорност на субјектите на критичната инфраструктура со CELEX бр.32022L2557.

Сектори на национална критична инфраструктура по правило се:

- Енергетика (производство, вклучувајќи и брани, рударство, пренос, складирање, транспорт на енергенсите и енергијата, дистрибуција и сл.);

- Транспорт (патен, железнички, воздушен и воден сообраќај);

- Банкарски системи и инфраструктура на финансиските пазари;

- Здравство (здравствена заштита, производство, трговија и контрола над лековите);

- Водоснабдување (системи за довод и одвод на води);

- Храна (производство и снабдување со храна, стокови резерви);

- Производство, складирање и превоз на опасни материи (хемиски, биолошки, радиолошки и нуклеарни материјали);

- Јавни служби (обезбедување на јавен ред и мир, заштита и спасување, итна медицинска помош);

- Дигитална инфраструктура, комуникациски и информациски технологии (електронски комуникации, пренос на податоци, информациски уреди и инсталации, аудио и аудиовизуелни медиумски услуги и сл.). [145]

[144] Исто.,
[145] Предлог на Закон за критична инфраструктура, 2022, достапен на https://portal.mdt.gov.mk/post-body-files/legislativa-mod-file-iCuk.pdf

Имајќи во предвид дека областа на критична инфраструктура побарува меѓусекторска соработка, неопходно е вклучување на повеќе министерства, регулаторни агенции и субјекти директни носители сопственици или управители на објекти од критична инфраструктура.

Што се однесува до заканите и ризиците врз критичната инфраструктура, потребна е сеопфатна анализа што треба да се заснова на три основни фактори, а тоа се: природните непогоди, техничко-технолошки инциденти и актите на незаконско постапување, вклучувајќи го и тероризмот. Во однос на инволвираните субјекти што треба да бидат носители на ваквите активности потребен е интегративен пристап со вклучување на:

− министерствата, агенциите и дирекциите што функционираат во рамките на државата;

− локалните власти;

− инфраструктурните оператори;

− релевантните субјекти кои ги третираат засегнатите критични инфраструктури;

− приватниот безбедносен сектор (агенции, Комора на Република Северна Македонија за приватно обезбедување);

− научната и експертската заедница;

− јавноста и особено делот на медиуми итн.[146]

Неопходно е да се воспостави мулти-секторска структура за владеење и управување со отпорноста на системот на критична инфраструктура, паралелно со потребата за подигнување на разбирањето за комплексноста, меѓузависноста и ранливоста на инфраструктурните системи со приоретизирање на напорите за градење на отпорност. Особено е важно да се воспостави дијалог и доверба помеѓу Владата и учесниците/операторите на критичната инфраструктура, но и партнерски однос во поделбата на одговорноста помеѓу јавниот и приватниот сектор, бидејќи добар дел од критичната инфраструктура е во приватна сопственост и се користи од приватните сопственици, а е мошне важна за функционирање на државата и создавање на високо ниво на отпорност на општеството.

[146] О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура,. стр.210достапно на: https://obezbeduvanje.org.mk/wp-content/uploads/2020/12/Zashtita-na-kriticna-infrastruktura-za-web.pdf, стр.79, посетено на 12/3/2026, стр.210

Критичната инфраструктура е клучна за опстанокот и развојот и треба да биде одраз на меѓу-секторска соработка, односно примена во пракса на се владиниот и се општествениот принцип. Секоја импровизација во сферата на заштитата и безбедноста на критичната инфраструктура која ќе се манифестира низ ненавремена, недоволна и несоодветна заштита ќе ја наруши безбедноста и отпорноста на истата и ќе претставува реален предизвик за нормално функционирање на општеството и реална закана за националната, регионалната и европската безбедност.

Имајќи во предвид дека странското сопственишство, контрола или директни инвестиции во критичната инфраструктура, финансискиот систем и/или други области претставуваат ранливост и со тоа безбедноста и стабилноста на Републиката се доведуваат во ризик, се наметнува потребата од задолжително воспоставување на национален механизам за проверка на странски директни инвестиции за справување со потенцијалните ризици по безбедноста и јавниот ред и мир, поврзани со странските директни инвестиции.

Регулативата за координација за проверка на странските директни инвестиции на ЕУ[147] има за цел обезбедување безбедност и јавен ред и мир во рамките на ЕУ а дополнително, се работи и за нашата сопствена национална безбедност и јавниот ред и мир како земја членка на НАТО и земја која официјално ги започна пристапните преговори за полноправно членство во ЕУ. Во оваа насока Република Северна Македонија неминовно ќе треба да ги изгради и да ги прилагоди сите свои политики, системи и механизми за да може целосно да го „затвори“ својот територијален простор и да го заштити од пенетрација на корозивен, сомнителен, штетен капитал. Регулативата за проверка на странските директни инвестиции е дел од пристапните преговори и според правилата на Договорот за основање на ЕУ, таа ќе биде директно применлива и за нас со денот на нашето членство во ЕУ. Регулативата е сложена и нејзината важност постојано расте во светот кој неминовно се менува. [148]

Како земја која ги започна пристапните преговори во јули 2022 година, на билатералниот скрининг за Поглавјето 30 Надворешни односи (дел од Кластер 6) веќе презедовме обврска за дефинирање на национален систем и правно решение за проверка на странските директни инвестиции, кој ќе се гради на инклузивен начин со сите засегнати страни и меѓународната заедница. Ова е нотирано и во Скрининг извештајот за Кластер 6, каде Комисијата нотира дека планира да донесе законодавство до крајот на 2025 и да има функционален систем во 2026 година. Обврската е поврзана и со заложбите во рамките на Берлинскиот процес, бидејќи на последниот Самит се донесе

[147] https://policy.trade.ec.europa.eu/news/revision-eus-foreign-investment-screening-mechanism-2025-12-11_en, посетена на 12/3/2026
[148] https://ekonomijaibiznis.mk/ тилев-механизам-за-проверка-на странс%d1%82%d0%b8%d0%bb%d0%b5%d0%b2?IdNews=26331, посетена на 29/3/2026

документ за регионални критериуми за воведување на национален механизам за скрининг на странските директни инвестиции. И конечно механизмот за скрининг на странски директни инвестиции претставува интегрален дел од Стратешкиот дијалог помеѓу Северна Македонија и САД. Воспоставувањето на национален механизам за скрининг на странските директни инвестиции е особено важно за Северна Македонија, не само како потврда дека националните политики ги следат трендовите и политиките на нашите стратешки партнери ЕУ и САД, туку и како потврда дека државата има капацитет да воспостави правна и институционална рамка за справување со потенцијалните ризици по безбедноста и јавниот ред и мир, поврзани со странските директни инвестиции. Задачата на формираната Работна група е разработка и предлог на правно решение за воспоставување на функционален национален систем за проверка на странските директни инвестиции, кој ќе биде компатибилен со националните системи за проверка на странските инвестиции на земјите членки на Европската Унија и во корелација со Регулативата на ЕУ за механизам за координација на скрининг на Странските директни инвестиции (СДИ 2019/452). [149]

Законското и институционално решение треба да биде во согласност со Регулативата (ЕУ) 2019/452 на Европскиот парламент и на Советот од 19 март 2019 година за воспоставување Механизам за скрининг на странски директни инвестиции во Унијата, и дефинициите и критериумите кои се утврдени во оваа Регулатива. Механизмот има две нивоа, првото е национален механизам за скрининг (проверка и верификација на странските директни инвестиции), а второто (Регулативата 2019/452) е способност на националниот механизам за скрининг на странските директни инвестиции за координација со сите членки на ЕУ и со Европската комисија. Главната цел е заштита на безбедноста и јавниот ред и мир, на национално ниво, но и ниво на ЕУ, а како членка на НАТО и на ниво на сите земји членки на НАТО. Регулативата се фокусира на широк спектар на сектори, вклучувајќи критична инфраструктура, критични технологии, синџири на снабдување и чувствителни податоци.

Препорачливо е да се направи длабинска анализа на приливот на странски директни инвестиции во Северна Македонија, особено во стратешките сектори (на пр. енергетика, транспорт) или во средства (технологии и инпути поврзани со стратешки сектори, критична инфраструктура во секторите, чувствителни податоци) што може да предизвика загриженост во областите како што се безбедност, јавен ред и/или контрола

[149] https://mep.gov.mk/mk-MK/transparentnost/novosti/mep-murtezani-na-konstitutivnata-sednica-na-rabotnata-grupa-za-vospostavuvanje-na-model-za-nacionalen-mexanizam-za-proverka-na-stranskite-direktni-investicii, посетена на 29/3/2026

на критичните средства, особено кога инвеститорот е во сопственост или е контролиран од трета земја, или има корист од значителни државни субвенции.[150]

Се работи на законско решение за пријавување и проверка на странски директни инвестиции со цел: воспоставување на транспарентна и ефикасна процедура за пријавување и проверка на странски директни инвестиции; идентификување и проценка на потенцијалните ризици од странски директни инвестиции за националната безбедност, јавниот ред и стратешките интереси; донесување на образложени одлуки во врска со потенцијалните странски директни инвестиции; зајакнување на правната сигурност за странските инвеститори и трговските друштва во Република Северна Македонија; и спречување на странски директни инвестиции од странски инвеститори кои се предмет на санкции или други рестриктивни мерки донесени од страна на Советот за безбедност на Обединетите Нации и Европската Унија.[151]

Заради заемен интерес и транспарентност при градењето на вакви осетливи политики и решенија, Владата треба навремено да ја информира, но и да ја вклучи деловната заедница преку претставници од сите стопански комори и од Советот на странски инвеститори кои работат во земјава. Неопходно е економските оператори да ја разберат во целост и правилно потребата и користа од прифаќање на Регулативата за проверка на странски директни инвестиции, секако во моментот кога ќе бидат воспоставени сите законски и институционални предуслови, за да се обезбеди ефективна соработка и координација со механизмот на ЕУ за странски директни инвестиции, како и со механизмите за проверка на странските директни инвестиции на другите стратешки партнери како што се Соединетите Американски Држави, Обединетото Кралство и други.[152]

5. Напори за зајакнување на сајбер безбедноста и справување со закани од лажни бомби

Динамичниот развој на информациско-комуникациските технологии и нерамномерната дигитализација на процесите во различни димензии на општеството значително ја менува перспективата за сајбер безбедноста и го зголемува ризикот од сајбер напади и сајбер инциденти. Безбедна, отпорна и доверлива дигитална трансформација на процесите, и на општеството во целина, може да се постигне само доколку е поставена на солидни основи, во сигурен и отпорен сајбер екосистем.

[150] Јовановски З., Мизо В., Тилев Д., Механизам за скрининг на странски директни инвестиции во Северна Македонија - Зошто и како?, Студија за политика, 2022, стр.33
[151] Согласно задачата на Работната група за воспоставување на модел за национален механизам за проверка на странските директни инвестиции
[152] Јовановски З., Мизо В., Тилев Д., Механизам за скрининг на странски директни инвестиции во Северна Македонија - Зошто и како?, Студија за политика, 2022, стр.34

Република Северна Македонија, како и другите држави, се соочува со ранливост од сајбернапади насочени против клучни сектори какви што се инфраструктурата, владата, образованието и бизнисот, кои предизвикуваат прекини во услугите и економски штети. Пример за ова се DDoS (Distributed Denial of Service) нападите врз веб-страницата на Државната изборна комисија за време на изборите во јули 2020 година, заканите пратени преку е-пошта за поставени бомби во 76 образовни и 42 други институции во 2023 година и нападите со уценувачки софтвер (ransomware) врз државни институции (Фондот за здравствено осигурување во 2023 година).[153]

Во дигиталната ера, сајбер безбедноста е основен столб на националната безбедност, на економскиот раст и на општествената отпорност. Стратегијата за сајбер безбедност 2025 - 2028 година ја одразува посветеноста на Владата на Република Северна Македонија да гради безбедна и отпорна дигитална средина, како интегрален елемент од процесот на целосна дигитална трансформација на општеството. Стратегијата за сајбер безбедност 2025 - 2028 година се предлага во насока за континуитет на заложбите на Владата на Република Северна Македонија во областа сајбер безбедност. Во согласност со Законот за изменување и дополнување на Законот за организација и работа на органите на државната управа, член 26-а, (Службен весник на Република Северна Македонија“ бр. 121/24), Министерството за дигитална трансформација има надлежности во областа безбедност на мрежи и информациски системи.[154]

Стратешкиот приоритет на Владата на Република Северна Македонија го вклучува јакнењето на сајбер безбедноста и отпорноста на институциите, со цел заштита на критичната инфраструктура и јакнење на довербата во јавните служби. Дополнително Законот за безбедност на мрежи и информациски системи, содржи јасни правни аспекти и дава насоки за делување во сајбер просторот, истиот е во согласност со ЕУ и НАТО директивите.

Стратегијата за сајбер безбедност 2025 - 2028 година и Стратегијата за градење отпорност и справување со хибридни закани 2021-2025 се комплементарни, бидејќи и двете препознаваат сајбер-нападите како клучен инструмент на хибридните закани. Хибридните закани, често таргетираат критични инфраструктури преку сајбер-просторот, вклучувајќи сектори со висока критичност. Стратегијата за сајбер безбедност 2025 - 2028 година се фокусира на градење силен национален сајбер екосистем преку јакнење на институционалните капацитети, подобрување на одговорот на инциденти и поттикнување на јавна и приватна соработка. Од друга страна, Стратегијата за хибридни закани го вклучува сајбер-просторот како клучна компонента во заштитата на

[153] НАЦИОНАЛНА РАЗВОЈНА СТРАТЕГИЈА 2024 – 2044, стр.73
[154] Стратегија за сајбер безбедност 2025 – 2028, стр.7, достапна на: https://mdt.gov.mk/files/sodrzina_na_CCB_2025_2028_usoglasen_tekst.pdf, посетена на 15/02/2026

критичните национални сектори, нагласувајќи ја потребата од меѓународна соработка со НАТО и ЕУ за заедничко справување со сајбер и хибридните предизвици. [155]

Дополнително со Законот за безбедност на мрежи и информациски системи[156], се уредува безбедноста на мрежните и информациските системи, надлежните органи за безбедност на мрежните и информациските системи и управување со значајни сајбер безбедносни инциденти и сајбер безбедносни инциденти со голем опфат, единствената точка за контакт за сајбер безбедност, тимовите за одговор на компјутерски инциденти, мерките за безбедност на мрежни и информациски системи и за управување со ризикот за сајбер безбедност, обврските за известување за сите аспекти на безбедност на мрежни и информациски системи за правните лица кои обезбедуваат услуги во областите со висока критичност и другите критични области, правилата и обврските за известување и размена на информации за инциденти, обврската за усвојување на стратегија која ја опфаќа безбедноста на мрежните и информациските системи, надзорот над спроведувањето на одредбите од овој Закон, како и други прашања поврзани собезбедност на мрежни и информациски системи. [157]

Министерството за одбрана и Армијата на Република Северна Македонија ја третираат сајбер безбедноста како суштински елемент на современата одбрана и националната безбедност. Во рамки на институционалниот развој, поставени се темелите за воспоставување на посебни капацитети за сајбер одбрана, насочени кон заштита на критичната одбранбена ИКТ-инфраструктура и подобрување на оперативната подготвеност. Во тек е изработка на нова Стратегија за сајбер одбрана, која ќе ги дефинира приоритетите, одговорностите и механизмите за заштита на националната одбранбена инфраструктура во сајбер доменот.

Справување со лажни дојави за бомби- Case Study

Во согласност со анализата на Мета.мк за лажни дојави за поставени бомби во Република Северна Македонија (од 26 октомври 2022 до 02 март 2023 година) резултатот е следен биле опфатени осум градови, имало вкупно 905 лажни дојави за бомби, од кои 876 биле во основни и во средни училишта. Речиси третина од дојавите се случиле во среда, а најретко дојави имало во понеделник. Февруари бил месец на најмногу дојави – само пет дена во текот на училишната недела (без да се земат предвид викендите), немало лажна дојава за поставена бомба во објект на некое училиште.

[155] Исто.,стр.10
[156] Законот за безбедност на мрежи и информациски системи, СВ на РСМ, бр. 135 од 4.7.2025 година
[157] Со овој закон се врши усогласување со ДИРЕКТИВА (ЕУ) 2022/2555 НА ЕВРОПСКИОТ ПАРЛАМЕНТ И НА СОВЕТОТ од 14 декември 2022 година за мерките за високо заедничко ниво на сајбербезбедност низ Унијата, за изменување на Регулативата (ЕУ) бр. 910/2014 и Директивата (ЕУ) 2018/1972 и за укинување на Директивата (ЕУ)2016/1148 (Директива NIS) со CELEX број 32022L2555

Почеста цел биле основните отколку средните училишта. Заклучоците од лажните дојави за поставени бомби во земјава кои ги анализираше Мета.мк, беа во согласност со добиените податоци од Министерството за внатрешни работи, користејќи го Законот за слободен пристап до информации од јавен карактер. Од МВР била доставена листа на сите дојави за поставени експлозивни направи, до училиштата и до 42 други објекти на институции. Според бројките, произлегува дека имало вкупно 905 лажни дојави за поставени бомби, а евидентно е дека на дојавувачите најголема цел им биле училиштата и внесувањето страв и паника токму кај децата и кај нивните родители. [158]

Слика 3, извор: Инфографик: Мета.мк

Во согласност со протоколот на МВР јавноста повеќе не е информирана за тоа дали има дојави за подметнати експлозивни направи во основните и во средните училишта, но и во останатите објекти во земјава, освен ако за тоа не одлучат стручните лица. Новите протоколи беа донесени со цел паниката и нервозата во јавноста да се сведат на минимум, а секојдневието на учениците, наставниот кадар и на родителите да биде без непотребни стресови. Со усвојување на новите безбедносни протоколи се намали интензитетот на лажни закани за бомби со што се потврди нивната ефикасност. Дополнително следеа: Размена на информации и интервјуа со релевантни и засегнати државни институции; интензивна комуникација со јавноста; усвојување на предложените мерки и активности за ублажување на злоупотребата на јавно објавените електронски пораки на училиштата; препораки за развој на решение за портал за пошта

[158] Ова истражувачка сторија е подготвена како дел од проектот „Зголемување на граѓанското учество во Дигиталната агенда – ICEDA“

со филтрирани и ограничени функционалности; препорака до институциите за користење на службени мејл адреси за служена кмуникација.[159]

6. Справување со дезинформации, странско мешање и манипулирање со информаци во Република Северна Македонија

Хибридното војување од страна на малигни и непријателски актери во форма на сајбер напади, операции на влијание и дезинформации против цели во Западен Балкан е поттикнато од политичките, економските и социјалните услови во регионот. Ако политичката моќ е високо концентрирана, елитите се фракционализирани и одвоени од својот народ, и колку повеќе економскиот систем е под контрола на политичките елити, толку повеќе дезинформациите претставуваат безбедносна закана. Ако политичките и економските системи се поконкурентни, тогаш лажните вести стануваат помалку упорни. Понатаму, во државите што имаат силни етнички и религиозни поделби, како Северна Македонија и Босна и Херцеговина, општеството е попосакувана цел за непријателски и оцрнети актери.[160]

Република Северна Македонија како стратегиски позиционирана земја на Балканот, е изложена на различни форми на странско влијание, кои често вклучуваат манипулација со информации со цел да се наруши јавната доверба во институциите, да се генерира политичка нестабилност или да се попречи евроатлантската интеграција. Надворешните актери, користејќи напредни дигитални алатки, социјални мрежи и традиционални медиуми, сè почесто спроведуваат информативни операции со кои се таргетираат клучни сектори во државата. Покрај про-руските наративи кај некој медиум во македонскиот медиумски контекст дополнително се засилија и други линии на дезинформации – од анти-ЕУ и анти-НАТО пораки до манипулативни содржини поврзани со изборни процеси, здравствени теми и новите технологии, вклучувајќи ја и вештачката интелигенција.

Република Северна Македонија работи посветено на развој на сопствени капацитети за справување со хибридни закани, додека истовремено се развива и јавната свест и потребата од критичко размислување и препознавање на дезинформациите.

Иако напорите за спротивставување на дезинформациите се клучни за нашиот пристап против хибридното војување, подигнувањето на свеста на граѓаните да ги сфатат дезинформациите и медиумскиот пејзаж со кој се соочуваат, ќе помогне во намалување навлијанието на погрешните информации врз најранливите и ќе ги заштити демократските процеси каде е потребна граѓанска вклученост. Во Национална стратегија за безбедност на Република Северна Македонија 2024-2029 година е нотирана потребата од формирање координативно тело на централната власт составено од комуникатори од редот на: Канцеларијата на претседателот на Владата, Министерството за одбрана, заменикот на претседателот на Владата задолжен за економски прашања, Министерството за надворешни работи, Министерството за внатрешни работи, Министерството за образование и наука, Министерството за информатичко општество и администрација, Министерството за здравство и Министерството за животна средина

[159] https://metamorphosis.org.mk/shemata-na-laznite-dojavi-za-bombi-905-zakani-osum-gradovi-76-elektronski-adresi-infografik-novinska-agencija-meta-mk/, посетена на 12/3/2026

[160] Dolan C.J, HYBRID WARFARE IN THE WESTERN BALKANS: HOW STRUCTURAL VULNERABILITY ATTRACTS MALIGNED POWERS AND HOSTILE INFLUENCE, SEEU Review, 2022, стр.20

и просторно планирање. Ова тело треба да ги координира активностите на институциите за спротивставување на дезинформациите и да започне национална стратегија за справување со странските информациски манипулации и влијанија и дезинформациите како голем сегмент од истите. Ова тело треба да развие: ефективно партнерство со останати тела (како Советот за етика во медиумите, Синдикатот на медиумските работници и сл.) и граѓанскиот сектор во насока на заедничко дефинирање на проблемот со дезинформациите и начините на кои секој актер треба да делува во својот ресор; помагање и овозможување на саморегулацијата на медиумите; унапредување на медиумската писменост; промоција на начелата на слободно, објективно информирање преку почитување на новинарските стандарди и етички кодекси и зајакнување на професионалното новинарство. Не е можно ефикасно спротивставување со дезинформациите без активно учество на сите засегнати чинители во медиумскиот етер. Министерството за образование и наука понатаму ќе развие посебна програма за медиумска писменост за да се осигури дека нашите дипломци се медиумски писмени и го имаат во себе потребниот скептицизам кон оние кои креираат и распространуваат штетни и поделбени пораки.[161]

Напорите во справувањето со дезинформации имаат за цел:

- Справување со лажни дојави со закани за бомби;
- Справување со Ковид пропаганда;
- Борба против анти-НАТО, анти-ЕУ и руска пропаганда;
- Справување со дезинформации и мисинформации;
- Воведување на медиумска писменост во формално образование;
- Јавна дипломатија и градење на мрежа за дигитална дипломатија;
- Активно учество во мрежа на комуникатори на НАТО и на национално ниво.

Во таа насока, Кампањата на Институтот за комуникациски студии (ИКС) има за цел преку општествено делување, односно со вклучување на сите инволвирани страни (од безбедносен, одбранбен, медиумски и цивилен сектор) да се засили капацитетот на институциите за агилно откривање на овие закани и препознавање на дезинформациските кампањи пред тие да предизвикаат штета. Целта е заеднички да се укаже на штетните последици од ваквите софистицирани тактики и техники кои тешко се препознаваат, иако многу вешто го запоседнуваат јавниот простор, влегуваат во нашите домови преку мобилните телефони, преку културата, религијата, ги подриваат меѓуетничките односи, бидејќи тешко се препознаваат, битно е да ја изградиме таа отпорност како општество. Овие закани бараат координација и интегрирано делување — институционално, законодавно, медиумски и општествено. Во таа смисла, Комисијата за одбрана и безбедност и Комисија за транспорт, дигитална трансформација, животна средина и просторно планирање имаат одговорност да ги следат и анализираат овие процеси, но и да ги вклучат во поширокатa дебата за безбедноста на државата. Работата не се ограничува само на традиционалните теми поврзани со армијата или физичката безбедност – туку и на новите, нетрадиционални

[161] Национална стратегија за безбедност на Република Северна Македонија 2024-2029, стр.30

закани, меѓу кои токму информативната и комуникациската дестабилизација добива сè поголема тежина.[162]

Министерството за одбрана активно работи на развој на способности за справување со дезинформациите, првенствено преку системот за справување со дезинформации, во чии рамки се развива т.н. превентивна и образовна улога, заедно со функцијата на брзо и навремено откривање на дезинформациите и креирањето на систем за брз одговор на детектираните дезинформации.[163] Носител на овој систем е Секторот за информации и комуникации (со проактивна и реактивна функција) и Секторот - Регионален центар за односи со јавноста (со превентивна функција). Во согласност со Концептот за развој на систем за справување со дезинформации, превентивната функција се фокусира на развојот на медиумската писменост преку организација и реализација на обуки и курсеви, како и преку блиска соработка со Министерството за образование и наука, академската заедница и невладиниот сектор. Превенцијата вклучува и реализација на семинари и работилници со претставниците на медиумите со цел зголемување на разбирањето за одбранбената област, како и соработка со факултетите за новинарство и односи со јавноста. Проактивната функција се однесува на континуирано продуцирање на информативен материјал кој ќе овозможи ефикасно справување со дезинформациите, навремено планирање за можна појава на дезинформации, организација на т.н. „настани во заедницата“ со цел доближување на одбранбените активности до граѓаните, како и вмрежување со националните, НАТО и ЕУ капацитети за справување со дезинформации (т.н. „fact-chekers“). Реактивната функција првенствено значи сеопфатен медиумски мониторинг и креирање на систем за брз проток на информации за постоење на одредена дезинформација (брз систем на известување во рамки на Министерството и Армијата). Во Министерството за одбрана функционира систем на брзо информирање за детектирана вест и нејзино спроведување до раководството. Користејќи ги дигиталните комуникациски алатки, секоја вест со негативна конотација и потенцијал да се дефинира како дезинформација ефикасно се проверува, како појдовна точка за следните активности во доменот на односите со јавноста. Развојот на капацитетите на Министерството и Армијата во доменот на стратешките комуникации е еден од врвните приоритети, особено во доменот на развојот на лицата за нивна реализација. Регионалниот центар за односи со јавноста, во согласност со годишните планови за обука, континуирано спроведува курсеви за односи со јавноста. Овој Центар се фокусира и на развојот на капацитети и човечки потенцијал со познавања во областа на справувањето со дезинформациите, за што беше развиен и Курс за справување со дезинформации и градење на отпорност. [164]

За да се превенира странското мешање и да се минимизираат штетите од манипулирање со информациите, тоа вклучува и креирање на респонзивни институции за брзо откривање и разобличување на странското манипулирање и координирана акција за нејзино спречување. Темата добива на интензитет со развојот на новите технологии и употребата на сè пософистицирани напади преку дезинформации, сајбер криминал и хибридни закани кои потешко се препознаваат, а се ризични за демократијата, ги

[162] https://samoprasaj.mk/naacik/otvorena-institucionalna-debata-za-spravuvanje-so-stransko-vlijanie-i-manipuliranje-so-informacii/, посетена на 12/3/2026
[163] https://portal.mdt.gov.mk/post-body-files/strateski-dokumenti-mod-file-T8Mp.pdf, посетена на 12/3/2026
[164] Комуникациска стратегија на Министерството за одбрана 2025 година, стр.15

нарушуваат меѓуетничките односи, ја намалуваат довербата во институциите и ја нарушуваат општата безбедност.

Преку стратегиски пристап што вклучува институционално зајакнување, законски реформи, медиумска отпорност, јавна едукација и меѓународна соработка, државата може да ја намали ранливоста на странското мешање и манипулирање со информации и да го зајакне демократскиот капацитет за одбрана од хибридни закани.

Дополнително, следен чекор во развојот на мониторингот на медиумите и сите останати стеикхолдери како креатори на јавно мислење и на соодветна перцепција во јавноста за прашања поврзани со одбраната и безбедноста е изработка на методологија и дефинирање на алатки за истражување на информациската средина како столб на кој почива справувањето со дезинформациите, странското влијание и манипулациите со информации. Значајна улога на тој план има и ЦИВИЛ – Центарот за слобода, кој својата клучна мониторинг-единица за дезинформации и пропаганда, ја преименува во Тим на Цивил за мониторинг на хибридни закани (Civil Hybrid Threats Monitoring – CHTM), Овој тим повеќе не е само за следење на лаги во медиумите, тој ќе го отсликува проширениот мандат кој вклучува детекција, анализа и разобличување на дезинформации, странски операции на влијание, сајбер манипулации и напади, политичко мешање, говор на омраза и други компоненти на хибридното војување. Тоа значи директно соочување со софистицираните и често координирани напади врз вистината, мирот и стабилноста. Тимот на ЦИВИЛ за мониторинг на хибридни закани ќе работи преку различни платформи, јазици и региони за да идентификува и разобличи шеми на манипулација и операции на влијание. Обемот на тимот ќе опфаќа широк спектар на хибридни закани – од дезинформации и пропаганда до политичко мешање и говор на омраза, како и комплексни операции на хибридната воена закана. Како дел од својата проширена мисија, тимот ќе ја продлабочи соработката со регионални и меѓународни партнери, вклучувајќи го учеството во Глобалната иницијатива за одбрана на демократијата, Вестминстер Алијансата за Украина, и други иницијативи усогласени со ЕУ за спротивставување на авторитарното влијание. Единицата, исто така, ќе вклучува алатки со вештачка интелигенција, техники за анализа на податоци и механизми за прекугранична размена на информации за подобро следење на хибридните операции и злонамерните актери.[165]

Истражувањето „Ефектот на дезинформациите и странските влијанија врз демократските процеси во Северна Македонија во 2025 година“ спроведено од Фондацијата „Метаморфозис“ со поддршка од глобалната мрежа за одбрана и промоција на слободно изразување IFEX, како дел од сеопфатните напори има за цел да се

[165] ЦИВИЛ – Центар за слобода , https://civilmedia.mk/tsivil-objavi-proshiruvane-na-mandatot-na-svojata-kluchna-monitoring-edinitsa-za-monitoring-na-hibridnite-zakani/ посетена на 25/3/2026

разоткрие влијанието на странската пропаганда во Република Северна Македонија и преку јавна едукација да се зајакне капацитетот на клучните засегнатите страни (граѓански организации и активисти, медиуми и новинари, државни институции и носители на одлуки) за тие да може да земат активно учество во градењето отпорност на штетните антидемократски влијанија.[166]

Воспоставувањето национален модел за справување со странско мешање и манипулирање со информации ќе овозможи интегриран, функционален и одржлив систем со институционален одговор кон ваквите закани. Во документот за јавна политика „Институционален одговор на странско мешање и манипулирање со информации во Северна Македонија“, изработен од Институтот за комуникациски студии, главната порака е дека наместо интегриран систем, имаме мозаик од добронамерни, но често изолирани иницијативи. Анализата покажа дека Потребен е национален механизам за координација и отпорност, кој ќе обезбеди: јасно дефинирани улоги (кој што прави, кога и како); уредени протоколи за размена на информации помеѓу институциите; системско следење на ризиците и заканите; усогласена и транспарентна комуникација со јавноста. Манипулирањето со информациите од страна на странски служби директно или преку прокси-актери претставува сериозен предизвик за институциите во Република Северна Македонија. Во услови на засилена геополитичка конкуренција и дигитализацијата силен институционален капацитет за справување со странското мешање и манипулирање со информации е навистина неопходен. [167]

Појдовната студија за странско мешање и манипулирање со информации во Република Северна Македонија од 2005 година, препорачува мултидимензионален пристап што вклучува зајакнување на институционалните капацитети за детекција и одговор на дезинформациите, деполитизација на професионалниот безбедносен сектор и јавната администрација, подобрување на регулативите за отчетност, транспарентност и интегритет на медиумите, како и подигнување на јавната свест преку едукација за медиумска и информациска писменост. Од особено значење е и засилената соработка со меѓународните партнери, особено со НАТО и ЕУ, заради споделување информации, добри практики и технички капацитети за справување со овој тип хибридни закани.[168]

[166] Ефектот на дезинформациите и странските влијанија врз демократските процеси во Северна Македонија во 2025 година, Фондација за интернет и општество Метаморфозис – Скопје 2025 г., стр.5 https://metamorphosis.org.mk/wp-content/uploads/2026/03/efektot_na_dezinformaciite_2025.pdf, посетена на 25/3/2026

[167] Грижев А., Поповска В., Институционален одговор на странско мешање и манипулирање со информации во Северна Македонија, 2025, https://iks.edu.mk/wp-content/uploads/2025/11/institucionalen-odgovor-na-smmi_mk.pdf, посетена на 12/3/2026

[168] Хаџи-Јанев М.,Стоилковски М., Странско мешање и манипулирање со информации во Република Северна Македонија, Институт за комуникациски студии, Скопје 2025, стр.66-67

Заклучок:

Република Северна Македонија како земја кандидат за членство во ЕУ и членка на НАТО е изложена на сè поразновидни хибридни закани, кои се манифестираат преку координирани активности што комбинираат сајбер напади, дезинформации, странско влијание, економски притисоци и потенцијални закани кон критична инфраструктура. Особено ранливи се секторите како енергетиката, финансиските системи, јавните набавки, комуникациските мрежи и информативниот простор. Овие активности се насочени кон поткопување на националната стабилност, економската независност, довербата на јавноста во институциите и демократијата

Хибридните инструменти кои притоа се користат имаат за цел влијание врз демократските процеси, политичката стабилност и евроатлантските интеграции. Воениот елемент, иако индиректен, се манифестира преку информациско војување, зголемено воено присуство на трети актери во регионот, како и преку искористување на конфликти за дестабилизација на довербата кон НАТО и ЕУ. Единствениот ефикасен одговор во справувањето со хибридните закани е проширувањето на пристапот кон безбедноста и тоа на заеднички и здружен начин со сите чинители во општеството и со нашите сојузници.

Примарната одговорност за справување со хибридните закани е на национално ниво, но често хибридните закани ги надминуваат националните граници, што ја прави мултилатералната соработка неопходна. Природата на заканата значи дека државите треба да работат заедно со сојузниците и партнерите.

Во насока на унапредување на справувањето со хибридните закани потребна е подобра институционална координација и капацитет за рано препознавање и одговор на хибридни закани. Свесноста за ситуацијата, која вклучува рано откривање на закани и предизвици, може да помогне да се предупредат носителите на одлуки за областите каде што одвраќањето е неопходно. Овие области се разликуваат меѓу нациите, бидејќи имаат различни силни и ранливи страни, па затоа се побарува од секоја нација да спроведе искрена самопроценка на ранливостите. Подготвеноста за ваков вид закана во нејзината најрана фаза е од клучно значење за национално справување со овие закани.

Дополнително, потребно е да се развие заедничка стратешка култура низ целата влада и да се надминат бирократските ранливости, кои често се посочуваат како една од најзначајните слабости. Стратешката култура за министерствата за одбрана, размислувањето и дејствувањето во однос на одвраќањето е секојдневна работа, но за многу други делови од владата тоа е предизвик. Скринингот на странските директни инвестиции, правилата за транспарентност за невладините организации, трговските договори и многу други алатки обично се размислуваат само во однос на нивната

примарна намена. Но, тие алатки, кога се користат во оркестрирана национална акција, можат да послужат и за одвраќање на одреден непријателски актер. Користењето алатки во сите сектори е фундаментален елемент на ефикасно одвраќање од хибридни закани каде пристапот на целата влада и меѓувладината соработка е клучна за националната политика, помагајќи во ефективното споделување информации и донесување одлуки, имплементација и проценка.

Во плановите за градење отпорност на општеството треба да се вклучи инфраструктурата, енергетскиот и комуникацискиот систем, системите за снабдување со храна и вода, климатските промени, како и будно да се следи технолошкиот развој. Во справувањето со хибридните закани, во сите критични области, неопходно е да се работи на подигање на свесноста за значењето на критичната инфраструктура.

Со донесувањето на предлог Законот за критична инфраструктура, ќе може да ја заштитиме критичната инфраструктура во Република Северна Македонија, при што, важно е да се нагласи дека дефинирањето на националната критична инфраструктура не е конечен процес, туку е динамички и проактивен.Така што критичната инфраструктура и нејзиното дефинирање може да биде предмет на промена во согласност со проценките за ризици на секоја национална влада.

Една од најсериозните закани за демократскиот развој и стабилноста на нашата држава претсавува странското мешање и манипулацијата со информации. Како преку обиди за влијание врз изборни процеси или политички одлуки, така и преку настојувања за длабинско менување на јавното мислење, поткопување на довербата во институциите и создавање на општествена поларизација. Ваквите влијанија, кои често делуваат преку добро организирани мрежи со поддршка од странски актери, ја користат слабоста на медиумскиот систем, ниското ниво на медиумска писменост и недоволната координација меѓу државните институции и граѓанското општество. Затоа Република Северна Македонија треба да развива долгорочни политики, да инвестира во медиумската писменост и да ја поттикне соработката меѓу државата, образовниот систем и граѓанскиот сектор. Медиумската писменост како прва линија на одбрана од дезинформациите, веќе ја препознаа искусните демократии вградувајќи ја во образовните и јавните кампањи.

Стратегијата за градење отпорност и справување со хибридни закани и Акцискиот план 2021-2025, како прв чекор на патот кон градење на отпорност, е единствена национална рамка за координирање на одговорот кон хибридните закани во Република Северна Македонија. Тие претставуваат „пристап на целата влада“, продлабочувајќи ја соработката со НАТО и ЕУ и подобрувајќи ја свеста за ситуацијата преку зајакнување на работата на нашите разузнавачки служби и прилагодување на

вежбите на вооружените сили за ефикасно реагирање на хибридни закани, подобрување на отпорноста преку справување со потенцијални стратешки и критични сектори како што се сајбер безбедноста и критичните инфраструктури, заштитата на финансискиот систем и заштитата на јавното здравје. Стратегијата е со важност до декември 2025 година, а имајќи ги во предвид предизвиците од новиот безбедносен контекст, потребно е донесување на нова Стратегија која би требало да биде сеопфатна и да ги вклучува искуствата од научените лекции, посебно во делот на реализацијата, во координација со релевантните институции и меѓународни партнери.

Советот за координација на безбедносно-разузнавачката заедница треба да го иницира процесот на ажурирање на Стратегијата и придружниот акциски план преку: реорганизација на системот и алатките за спроведување на Стратегијата во делот на надлежностите на назначените институции како носители на активноста; редефинирање на задачите и временските рокови; обезбедување на ресурси за институциите назначени за спроведување на активноста; унапредување на соработката со надлежните институции од стратешките партнери во рамките на Европската Унија и НАТО (Европскиот центар на извонредност за борба против хибридни закани; Сајберцентарот за извонредност на НАТО; НАТО центарот за извонредност во стратегиски комуникации).[169]

Бенефитот од добро изграден систем и воспоставена широка соработка, ќе значи отпорно општество на новите безбедносни предизвици, безбедни институции, општествена свест и подготвеност за заштита и безбедност на граѓаните и општествените добра. Клучниот овозможувач на безбедност и општествена отпорност се свесноста и подготвеноста на сите да преземат удел во одговорноста за нивната сопствена безбедност, како и за безбедноста на другите.

Нашиот фокус е да негуваме општество што не само што ќе ги издржи шоковите од кризите и од катастрофите, туку и ќе се истакне во превентивното и проактивното управување со ризици и градењето отпорност. Ова ќе биде постигнато преку препознавање на системските ризици и искористување на научените лекции и искуствата за да ги подобриме превентивните мерки и одговори. За таа цел, ќе бидат спроведени детални и сеопфатни процени на ризик во различни сектори на национално и локално ниво, развивајќи стратешки испреплетени стратегии, политики и акции информирани за ризикот, при што родовата перспектива и попреченоста се вклучени и се интегрален дел од пристапот за намалување ризици од катастрофи, зајакнувајќи ја координацијата и подобрувајќи ја соработката помеѓу надлежните институции и субјектите коишто учествуваат во намалувањето на ризиците и обезбедувајќи

[169] Национална стратегија за безбедност на Република Северна Македонија 2024-2029, стр.20

вклученост на сите во општеството, а со цел да се подобрат капацитетите за превенција, подготвеност, одговор и закрепнување.[170]

Општествената отпорност подразбира оспособување на поединечните граѓани и граѓанското општество како целина да ги играат своите соодветни улоги за време на природни катастрофи, но исто така и низ целиот спектар на конфликти - од мир и криза до војна. Иако силните вооружени сили се неопходни за безбедноста на Алијансата, тие се потпираат на отпорно граѓанско општество како прва линија на одбрана. Вооружените сили, исто така, имаат важна улога во развојот на заеднички пристап на целото општество преку учество во заедничко планирање, споделување информации, образование, обука и вежби. Овој заеднички цивилно-воен пристап ја зајакнува отпорноста, гради доверба и го зголемува заедничкото разбирање.[171]

[170] НАЦИОНАЛНА РАЗВОЈНА СТРАТЕГИЈА 2024 – 2044, стр.68, Сл.весник на РСМ, бр. 222 од 31.10.2024 година
[171] NATO RESILIENCE SYMPOSIUM, 25-27 APRIL 2023, RIGA, LATVIA, стр.20

Литература:

1. О.Бакрески, Т.Милошевска, Ѓ.Алчески, Заштита на критична инфраструктура, Скопје 2017

2. Хаџи-Јанев М.,Стоилковски М., Странско мешање и манипулирање со информации во Република Северна Македонија, Институт за комуникациски студии, Скопје 2025.

3. Митревска М., Милески Т.,Кон отпортност и заштита на критичната инраструктуа: студија на случај на Република Северна Македонија, Скопје, 2022.

4. Попоска В., Информирана одбрана, Вовед за хибридните закани за критичната инфраструктура, Скопје, 2024.

5. Грижев А, Фрагментирани институции, силни манипулациски кампањи: зошто ни треба интегриран одговор

6. Јовановски З., Мизо В.и, Тилев Д., Студија за политика: Механизам за скрининг на странски директни инвестиции во Северна Македонија -Зошто и како?, Скопје, 2022.

7. Trojachanec M, Rizaov G, Metamorphosis Foundation:Analytical report on the Foreign Information Manipulation and Interference (FIMI) in the Republic of North Macedonia.

8. Стратегија за градење отпорност и справување со хибридни закани, април 2021

9. Национална стратегија за безбедност на Република Северна Македонија 2024-2029

10. Законот за безбедност на мрежи и информациски системи, СВ на РСМ, бр. 135 од 4.7.2025 година

11. Предлог на Закон за критична инфраструктура

12. НАЦИОНАЛНА РАЗВОЈНА СТРАТЕГИЈА 2024 – 2044, Сл.весник на РСМ, бр. 222 од 31.10.2024 година

13. НАЦРТ СТРАТЕШКИ ПЛАН НА ЦЕНТАРОТ ЗА УПРАВУВАЊЕ СО КРИЗИ ЗА ПЕРИОД 2025 – 2027 ГОДИНА, Скопје, август 2024 година

14. NATO, Warsaw Summit Communiqué, July 9, 2016

15. Resilience, civil preparedness and Article 3

16. A Global Strategy for the European Union’s Foreign And Security Policy, June 2016

17. Joint Framework on countering hybrid threat a European Union response, 2016

18. Joint Communication to the European Parliament, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats

19. A Strategic Approach to Resilience in the EU’s external action. Joint Communication to the European Parliament and the Council. Brussels, 7.6.2017, JOIN(2017) 21 final

20. Repot on FIMI threats, March 2025

21. EU NATO Joint Declarations (2016, 2018 and 2023)

22. Ninth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017

23. Hybrid threats to critical infrastructure in the European Union. Selected Hybrid CoE analyses, 2025

24. ROMERO, A. Reflections on European defence and its identities: NATO and EU, competition or cooperation? IEEE Analysis Paper 50, 2024.

25. Communication from the Commision to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Region on the EU Security Union Strategy, 2020

26. EU (2008) Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

27. EU (2022) Directive 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

28. REGULATION (EU) 2019/452 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union

29.A Strategic Compass for Security and Defence, March 21, 2022

30.NATO 2022 Strategic Concept

31. JOINT WHITE PAPER for European Defence Readiness 2030

32. EU-NATO TASK FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE FINAL ASSESSMENT REPORT, JUNE 2023

33. AC/281-WP(2025)0043-REV7 (R) -The Defence and security related Investments definition.

34. PO(2025)0158) – Revised Strategy on NATO's role in countering hybrid actions.

35. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Military Mobility, 2025

36. HybridCoE (2023) Hybrid threats: A comprehensive resilience ecosystem

37. EUROPOL – "EU Terrorism Situation and Trend Report (TE-SAT) 2023"

38. Lasconjarias G, Larsen A,J., NATO's Response to Hybrid Threats, NDC Forum Paper 24

39. Keršanskas V., ‘Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats , 2020

40. Spatafora G,.NATO's 76th anniversary: What's the future of the alliance?, 2025

41. Hunter E.C, Berzina, K., NATO and Societal Resilience: All Hands on Deck in an Age of War, 2022.

42. Accardo G., Vaz S ., and Carnazza G, New EU FDI Regulation: striking the right balance?, 2025

43. Hadley N., Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework ‘DISARM’, Hybrid CoE Research Report 7, November2022

44. CIMIC Handbook, CIMIC Centre of Excellence (CCOE)

45. Ефектот на дезинформациите и странските влијанија врз демократските процеси во Северна Македонија во 2025 година, Фондација за интернет и општество Метаморфозис – Скопје, 2025

46. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G.,Hybrid threats: a comprehensive resilience ecosystem – Executive summary, Publications Office of the European Union, Luxembourg, 2023

Интернет страници:

47.https://obezbeduvanje.org.mk/wp-content/uploads/2020/12/Zashtita-na-kriticna-infrastruktura-za-web.pdf

48.https://respublica.edu.mk/wp-content/uploads/2025/05/stransko-meshanje-i-manipuliranje-so-informacii-vo-rsm.pdf

49.https://library.fes.de/pdf-files/bueros/skopje/19769.pdf

50.https://respublica.edu.mk/blog/javen-interes/fragmentirani-institucii-silni-manipulaciski-kampanji/

51.https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

52.https://www.nato.int/cps/en/natohq/topics_132722.htm Resilience, civil preparedness and Article 3

53.https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

54.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018

55.https://www.eeas.europa.eu/sites/default/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf

56.https://eeas.europa.eu/sites/eeas/files/join_2017_21_f1_communication_from_commission_to_inst_en_v7_p1_916039.pdf.

57.https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

58.https://data.consilium.europa.eu/doc/document/ST-10471-2024-INIT/en/pdf

59.https://doi.org/10.4467/27204383TER.25.017.21520

60.https://www.ieee.es/Galerias/fichero/docs_analisis/2024/DIEEEA50_2024_ABEROM_OTAN-UE_ENG.pdf

61.https://www.consilium.europa.eu/en/policies/defence-security/eu-nato-cooperation/

62.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605

63.https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:en

64.https://eurlex.europa.eu/eli/dir/2022/2557/oj#:~:text=Council%20Directive%202008%2F114%2FEC%20%284%29%20provides%20for%20a%20procedure,crossborder%20impact%20on%20at%20least%20two%20Member%20States

65.https://www.hybridcoe.fi/publications/hybrid-threats-a-comprehensive-resilience-ecosystem/

66.https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf

67.https://www.google.com/search?q=NATO%E2%80%99s+Response+to+Hybrid+Threats%2C+Guillaume+Lasconjarias+and+Jeffrey+A.+Larsen&rlz=1C1GCEA_

68.http://www.prespa-institute.mk/wp-content/uploads/2024/02/Informirana-odbrana.pdf

69.https://eda.europa.eu/news-and-events/news/2025/03/19/joint-white-paper-for-european-defence-readiness-2030

70.https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon

71.https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf

72.https://www.iss.europa.eu/publications/commentary/natos-76th-anniversary-whats-future-alliance

73.https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf

74. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452

75. https://www.ashurst.com/en/insights/new-eu-fdi-regulation-striking-the-right-balance/

76.https://www.gmfus.org/sites/default/files/202207/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf

77.https://metamorphosis.org.mk/izdanija_arhiva/stabilnosta-pod-zakana-fimi-vo-severna-makedonija/

78.https://portal.mdt.gov.mk/post-body-files/zakoni-mdt-file-n2xm.pdf

79.https://portal.mdt.gov.mk/post-body-files/nacionalni-strategii-file-O8IL.pdf

80.https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=77229

81.https://www.strategic-compass-european-union.com/

82.https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf

83.https://www.hybridcoe.fi/wpcontent/uploads/2022/11/20221129_Hybrid_CoE_Research_Report_7_Disarm_WEB.pdf,

84.https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf

85.https://defence-industry-space.ec.europa.eu/document/download/a5b639aa-4d77-44b8-9f98-6bc0e54be984_en?filename=Joint%20communication%20on%20Military%20Mobility.pdf

86.https://www.act.nato.int/wp-content/uploads/2024/02/NATO-Resilience-Symposium-Report-2023.pdf

87. https://www.sciencedirect.com/science/article/pii/S277274162400019X

88. https://www.fimi-isac.org/index.html

89.https://metamorphosis.org.mk/wpcontent/uploads/2026/03/efektot_na_dezinformaciite_2025.pdf

90. https://cuk.gov.mk/Uploads/CMCStrategicPlan/cmc_639080576499179165.pdf