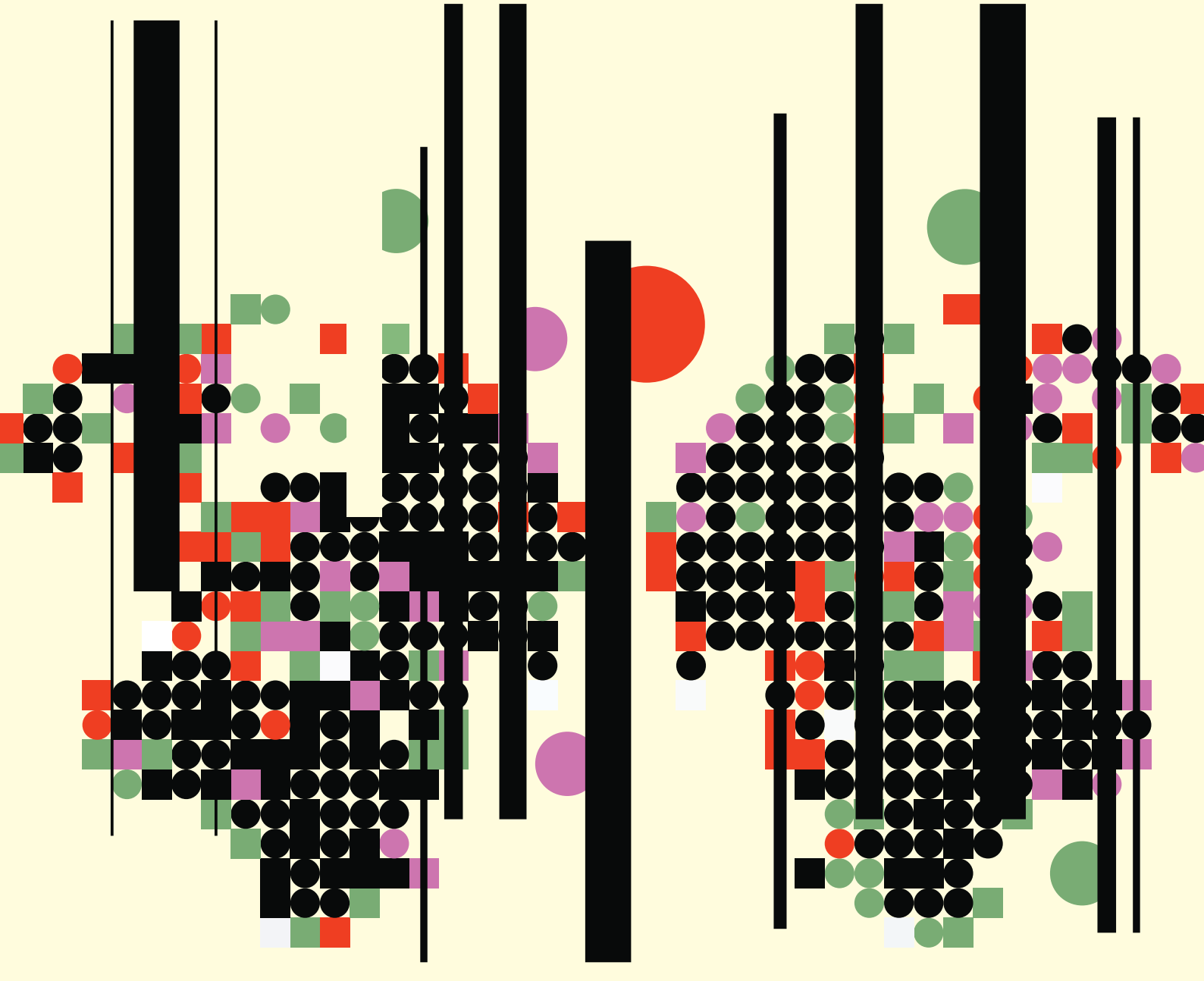
Институт за
комуникациски студии

Странско мешање и манипулација со информации (СММИ) во Северна Македонија: Основна проценка на институционалната подготвеност, рамките за координација и капацитетите за одговор



Скопје, 2026

Институт за комуникациски студии

respublica

Наслов::
Странско мешање и манипулација со информации (СММИ) во Северна Македонија: Основна проценка на институционалната подготвеност, рамките за координација и капацитетите за одговор

Издавач:
Институт за комуникациски студии (ИКС), Скопје

Автори:
Владимир Делов, Бојан Георгиевски, проф. д-р Жанета Трајкоска

Стручни рецензенти:
Џо МекКерон – Шипман, Служба за комуникации на Владата на Обединетото Кралство
Франческа Богери, ОБСЕ/ОДИХР
Федерико Џулио Сикурела, независен истражувач и консултант за СММИ
Весна Попоска, вонреден професор
Александар Грижев, вонреден професор

За издавачот:
проф. д-р Жанета Трајкоска

Дизајн:
Зоран Кардула

Графичко уредување:
Дејан Јовески

Лектура:
Симона Груевска-Маџоска

Издание:
РесПублика

Место и година:
Скопје, 2026 г.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека “Св. Климент Охридски”, Скопје

342.5:[316.776.23:327.8](497.7)(047.31)
[316.776.23:327.8]:34(4-672ЕУ:497.7)(047.31)

ДЕЛОВ, Владимир
Странско мешање и манипулација со информации (СММИ) во Северна Македонија [Електронски извор] : основна проценка на институционалната подготвеност, рамките за координација и капацитетите за одговор /
[Владимир Делов, Бојан Георгиевски, Жанета Трајкоска]. - Текст во PDF формат, содржи 29 стр., илустр. - Скопје : Институт за комуникациски студии, 2026. - (Едиција ResPublica)

Начин на пристапување (URL):
https://respublica.edu.mk/wp-content/uploads/2026/05/smmi-vo-makedonija-osnovna-procenka-na-institucionalnata-podgotvenost-ramkite-za-koordinacija-i-kapacitetite-za-odgovor-mk.pdf
(Слободен пристап). - Наслов преземен од екранот. - Опис на изворот на ден 26.05.2026. - Фусноти кон текстот. - Библиографија кон главите

ISBN 978-608-4805-87-8

1. Георгиевски, Бојан [автор] 2. Трајкоска, Жанета [автор]
а) Дезинформации -- Странски влијанија -- Институционален одговор -- Македонија -- Истражувања б) Дезинформации -- Странски влијанија -- Законско регулирање -- Европска Унија -- Македонија -- Истражувања в) Дезинформации -- Странски влијанија -- Истражувања

COBISS.MK-ID 68847621

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

Овој документ е подготвен во рамките на програмата „Зајакнување на оперативната подготвеност за одговор на државата кон странско мешање и манипулација со информации во Северна Македонија“, финансиран од Владата на Обединетото Кралство со поддршка на Британската амбасада во Скопје. Содржината на оваа публикација не мора нужно да ги одразува ставовите или мислењата на Владата на Обединетото Кралство.

Содржина

Поимник **4**

Вовед **5**

1. Правна и стратегиска рамка на Македонија за реагирање на странско мешање и манипулација со информации **7**

2. Анализа на законските надлежности на клучните институции во Северна Македонија **10**

Агенција за разузнавање 10

Агенција за национална безбедност 10

Министерство за одбрана и Закон за одбрана 11

3. Наоди од квалитативното истражување **11**

Резиме на констатациите за Македонија 15

4. Европска Унија: Градење заедничка рамка за борба против странско мешање и манипулација со информации **15**

Аналитички основи за разбирање на странското мешање и манипулација со информации: ABCDE 17

Циклус на анализа 19

Рамка DISARM 20

Матрицата на изложеност на странско мешање и манипулација со информации 21

5. RESIST 3: Пристапот на Обединетото Кралство во борбата против странско мешање и манипулација со информации **22**

Шесте чекори на RESIST 3 23

6. Следни чекори **26**

Библиографија **29**

Поимник

СММИ Странско мешање и манипулација со информации (СММИ) се однесува на незаконски тенденции на однесување што имаат потенцијал негативно да влијаат на вредностите, на процедурите и на политичките процеси. Таквата активност е манипулативна по својот карактер и се прави намерно и на координиран начин, и тоа од страна на државни или други актери, вклучувајќи ги тука и нивните претставници во и надвор од нивната територија.

Инцидент СММИ инцидент е дејство извршено од еден или од повеќе заканувачки актери со специфични цели и кои дејствуваат со намера да измамат. Дел од една кампања можат да бидат повеќе меѓусебно поврзани инциденти.

Кампања Сеопфатен збир од СММИ инциденти кои се започнати, во одреден временски период, против една или повеќе цели, а притоа општата цел е јасно зацртана и постои и потенцијален наратив.

ДММИ Домашното мешање и манипулирање со информации вклучува намерни кампањи кои се координирани на домашно ниво и честопати се применуваат со користење ботови, тролови и локални посредници за да се наруши јавното мислење, да се ослабне довербата во демократските институции и да се влијае врз изборите. Слични се на СММИ според техниката и намерата (манипулација со информацискиот простор во насока на поткопување на демократските процеси), но се спроведуваат од домашни актери, како што се локални политички партии, организации или поединци, и тоа против сопственото население.

ОМИ Операции за манипулација со информации – намерни, координирани кампањи кои имаат за цел да ја измамат публиката, да ја искриват реалноста и да влијаат врз перцепциите, однесувањето или одлуките, служејќи ѝ притоа на одредена агенда. Овие операции користат техники како што се ширење дезинформации, пропаганда и користење лажни профили со цел поларизирање на општествата и поткопување на довербата и тие честопати се вршат од странски актери.

Сива зона „Сива зона“ се однесува на непријателска активност која се наоѓа под прагот на директен конфликт помеѓу држави и има за цел да ја поткопа способноста на државите нормално да функционираат.

ТТП Тактики, техники и процедури што се користат од актерите кои вршат закани, со цел да се открие на кој начин се структурирани СММИ кампањите и како се извршуваат и приспособуваат со текот на времето.

Припишување Процес на идентификување на одговорни страни: се обидува да одговори на тоа „кој“ (држава, субјект поврзан со државата или посредник) стои зад координирана и измамничка информациска кампања, што честопати е тешко да се направи поради намерната употреба на посредници и техники на маскирање за да се избегне откривањето.

Тролање онлајн Тролањето онлајн е чин на намерно објавување провокативни, неискрени или пораки кои се надвор од темата, сето тоа во онлајн заедниците, а со цел да се провоцираат, да се вознемират или да се понижат другите. Троловите сакаат да поттикнат емотивни реакции или да предизвикаат нарушување чисто за лична забава и честопати дејствуваат анонимно и ги вознемируваат корисниците.

Вовед

Еволуцијата на современиот информациски пејзаж ја доведе Северна Македонија пред суштински важна крстосница. Хибридните закани, кампањите за странско мешање и манипулации со информации (СММИ) се аспекти кои сè повеќе се идентификуваат во националните стратегии како примарна закана за безбедноста и за демократската стабилност, и притоа преминот од нивното општо препознавање кон конкретна подготвеност на оперативно ниво е аспект кој и понатаму претставува значаен предизвик. Сегашните институционални одговори честопати се фрагментирани и тоа делумно поради тоа што се обидуваат да ги усогласат дефинициите кои се применуваат во политиките на високо ниво со хаотичната реалност на дигиталната средина во која вистинскиот идентитет на актерите честопати не е познат.

Во насока на надминување на оваа состојба, документот поаѓа од ставот дека, иако СММИ останува примарна стратешка грижа, оперативната влезна точка за институциите треба да биде поширокиот концепт на операции за манипулирање со информации (ОМИ). Овој пристап ја зема предвид основната реалност на информациската „сива зона“: во раните фази на еден инцидент, многу ретко може веднаш и со сигурност да се утврди дали станува збор за странско или за домашно мешање и манипулирање со информации (ДММИ), особено без форензички, технички или разузнавачки податоци. Затоа, доколку институциите го усвојат пристапот заснован на ОМИ, ќе се намали ризикот истрагите предвремено да се насочат кон погрешни аспекти или да бидат блокирани поради неможност веднаш да се припише активноста на конкретен актер. Со други зборови, идентификувањето на изворот треба да се третира како важна последователна фаза на анализата, а не како предуслов за почетно одбранбено дејствување.

Ваквата рамка им овозможува на институциите да се фокусираат најпрво на тоа како се спроведува манипулацијата, односно на тактиките, техниките и процедурите, наместо веднаш да се обидуваат да утврдат кој стои зад неа. Така, протоколите за реагирање може да се активираат навремено, без институциите да бидат парализирани од долготрајни постапки за дефинитивно припишување на активностите. Во овој контекст, припишувањето останува суштинска фаза на разузнавачката и на аналитичката работа, но не и предуслов за институционална реакција.

Сепак, специфичниот фокус на ова истражување и понатаму е цврсто на СММИ и ја одразува посветеноста на Северна Македонија кон усогласување на своите политики со евроатлантските безбедносни рамки. Иако границите помеѓу СММИ, ДММИ и општите кампањи за дезинформирање не се доволно јасни, и тоа е така поради нивната природа, странското мешање сепак претставува уникатна закана за националниот суверенитет што бара примена на специјализирани, дипломатски и стратешки контрамерки.

Целта на овој документ е да го премости јазот помеѓу стратегиската политика и практичното институционално постапување. Преку заедничка аналитичка основа која ја препознава флуидноста на информациските закани, документот нуди насоки за развој на стандардизирани координативни механизми, сеопфатни стандардни оперативни процедури (СОП) и специјализирани алатки за одговор на инциденти. Со тоа, документот треба да придонесе институциите во Северна Македонија да бидат подобро подготвени навремено, координирано и решително да реагираат на манипулативни информациски напади, без притоа да се занемари темелната анализа потребна за идентификување, изолирање и спротивставување на странското мешање.

Оваа анализа директно се надоврзува на три претходни публикации објавени од Институтот за комуникациски студии (ИКС), кои заеднички ја формираат базата на докази за тоа зошто е потребен еден поопеативен пристап. Прво, документот за јавна политика „Институционален одговор

на странското мешање и манипулација со информации во Северна Македонија: Модели и опции за политика“[1] дава квалитативен увид во тоа како институциите во моментов го разбираат странското мешање и манипулација со информации и како реагираат во пракса. Наодите укажуваат на неусогласеност во концептуализацијата на странското мешање и манипулација со информации во јавниот сектор, при што зрелоста на разбирањето е поизразена кај безбедносно-разузнавачката заедница, додека на државно ниво недостига единствен, кодифициран и институционално усогласен концепт. Клучниот заклучок е дека, и покрај постоењето на релевантни институции и индивидуални капацитети, сè уште отсуствува формализиран модел на меѓуинституционална соработка за инциденти поврзани со странско мешање и манипулација со информации, што резултира со реактивност и зависност од индивидуална иницијатива.

Второ, документот за јавна политика „Справување со СММИ во контекст на регулативите на ЕУ“[2] го позиционира институционалниот предизвик во динамичната европска регулаторна и политичка средина и ја разјаснува нормативната и практичната релевантност на пристапите во ЕУ на земјите кандидатки. Трето, анализата „Странско мешање и манипулација со информации во Северна Македонија“[3] обезбедува поширок контекст за состојбата во државата и дополнително ја потврдува оценката дека празнините во подготвеноста и координацијата имаат структурен, а не инцидентен карактер. Овие документи конвергираат кон една конзистентна констатација: ограничувањата не се сведуваат исклучиво на капацитети туку и на отсуство на предвидлив институционален „пат“ преку кој инцидентот се движи од откривање и иницијална проценка, преку донесување одлуки, до јавна комуникација и институционално учење.

Основната состојба и аналитичката рамка на овој документ се водени од следниве прашања: (1) Како функционираат во пракса меѓународно воспоставените аналитички рамки и рамките за реагирање на странско мешање и манипулација со информации, особено во рамките на Европската Унија и Обединетото Кралство? (2) Кои елементи од тие рамки се најрелевантни и применливи за институционалниот контекст на Македонија? (3) Каде се лоцирани клучните празнини помеѓу националните стратегии и секојдневната институционална реалност при реагирање на инциденти поврзани со странско мешање и манипулација со информации? (4) Како постојните задачи и капацитети можат да се поврзат во појасен и попредвидлив модел што овозможува координација, ескалација и одговор?

Методолошки, проценката се потпира врз квалитативно истражување и анализа на документација. Таа опфаќа преглед на клучни аналитички и оперативни рамки на ЕУ и Обединетото Кралство за справување со странско мешање и манипулација со информации, вклучително и ABCDE, циклусот на анализа на EEAS, DISARM, Матрицата на изложеност на странско мешање и манипулација со информации и RESIST 3, разгледани како институционални алатки, а не како апстрактни модели. Паралелно, Институтот за комуникациски студии спроведе полуструктурирани интервјуа со поранешни и актуелни високи јавни функционери, пратеници и државни службеници од релевантни институции, дополнети со консултативни дискусии во рамките на Координативното тело за странско мешање и манипулација со информации иницирано од Институтот за комуникациски студии. На овој начин беа прибрани емпириски согледувања на постојните практики за координација, институционални ограничувања и „тесните грла“ во процесите.

---

1 Институт за комуникациски студии (ИКС) (2025) Институционален одговор на странско мешање и манипулација со информации во Северна Македонија: Модели и опции за политика. Скопје: ИКС. Достапно на: https://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf

2 Институт за комуникациски студии (ИКС) (2025) Справување со СММИ во контекст на регулативите на ЕУ. Скопје: ИКС. Достапно на: https://respublica.edu.mk/wp-content/uploads/2025/06/policy-paper-addressing-fimi-in-context-of-eu-regulations-en.pdf

3 Институт за комуникациски студии (ИКС) (2025) Странско мешање и манипулација со информации во Северна Македонија (Основна студија). Скопје: ИКС. Достапно на: https://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf

Современите европски рамки нагласуваат пристап на ниво на „целото општество“, кој вклучува организации на граѓанското општество (ГО), медиумски субјекти и приватни технолошки компании, додека ова истражување намерно го стеснува својот фокус и ги зема предвид капацитетот на државата и на владата. Ваквото разграничување се заснова на претпоставката дека постоењето на сеопфатна основа која ја подразбира „целата држава“ е функционален предуслов за секоја поширока општествена мобилизација. Во контекст на Северна Македонија, институционалната фрагментација и понатаму претставува главна пречка; и од тие причини, оваа студија им дава приоритет на механизмите за внатрешна координација, законските овластувања и на оперативната подготвеност на државните институции.

Иако суштински важната улога на актерите кои не се дел од државниот апарат и потребата од ангажирање на контакт точки кај технолошките компании се нешта кои се препознаваат како долгорочни предности, тие сепак не се директно опфатени во опсегот на оваа анализа. Целта овде е да се направи проценка на институционалната основа на државата („прв одговор“ во услови на хибридни закани) пред овие поширок структури кои вклучуваат повеќе засегнати страни да можат ефикасно да се интегрираат. Следствено на тоа, полуструктурираните интервјуа кои беа спроведени за потребите на оваа студија беа со високи јавни службеници и со државни службеници со цел конкретно да се дијагностицираат внатрешните структурни празнини во рамките на државниот апарат.

Оваа основа не претставува стратегија за јавни политики, ниту ги заменува националните стратегиски документи. Таа служи како мост за операционализација: целта е да го поддржи развојот на реални координативни текови, стандардни оперативни процедури и обрасци на одговор на инциденти што се усогласени со стандардите на ЕУ и на партнерите, но истовремено се засновани на постојните институционални мандати и капацитети во Македонија.

1. Правна и стратегиска рамка на Македонија за реагирање на странско мешање и манипулација со информации

Република Северна Македонија формално ги препознава хибридните закани и операциите поврзани со информации како составен дел од националното безбедносно опкружување. Во Стратегијата за градење отпорност и справување со хибридни закани од 2021 година, како и во Стратешкиот одбранбен преглед за 2018 година, хибридните закани се дефинираат како координирана употреба на конвенционални и неконвенционални методи од страна на државни или недржавни актери за постигнување на стратешки цели. Овие закани комбинираат асиметрични, психолошки и киберелементи, ја искористуваат ранливоста во општеството и, конечно, имаат за цел да ја поткопаат довербата во демократските институции.

Клучната стратегиска референтна точка на Македонија е Стратегијата за градење отпорност и справување со хибридни закани за периодот 2021 – 2025 година, која експлицитно ги препознава информациските операции како сериозна закана и ги наведува медиумската манипулација, координираните мрежи на ботови и тролови и ширењето на дезинформации како типични инструменти на хибридна активност.

Ова стратегиско обликување обезбедува политичка и концептуална основа за подготвеност за странско мешање и манипулација со информации, третирајќи ја манипулацијата со информации како прашање на државна отпорност, а не како изолиран комуникациски проблем. Сепак, останува системското ограничување – стратегиските документи во значајна мера артикулираат што треба да постои (рано предупредување, координација, отпорност), но недоволно кодифицираат како во пракса институциите откриваат, проценуваат, ескалираат и управуваат со конкретни инциденти.

Правната рамка на Македонија не секогаш директно го користи терминот „странско мешање и манипулација со информации (СММИ)“, што е очекувано поради релативната новина на концептот, но правните основи најчесто се појавуваат преку поширок овластувања поврзани со заштита на суверенитетот, уставниот поредок, националната безбедност, спречување странска субверзија, справување со киберзакани и координација на безбедносно-разузнавачката заедница.

За операционализација на пристапот, стратегиската рамка дефинира приоритети, меѓу кои: (1) Развој на систем за рано предупредување и известување за информациски операции во координација со експертизата на ЕУ и НАТО; (2) Зајакнување на медиумската писменост и критичкото размислување преку улогата на граѓанското општество; (3) Развој на способности за откривање на дезинформации, психолошки операции и координирано онлајн тролање.

Воедно, се артикулира тријада на методи: рано откривање на закани, градење отпорност со цел намалување на штетата и ефикасен процес на одговор на стратешко ниво под водство на националните координативни структури, при што се нагласува дека базична подготвеност треба да развијат и сите министерства, а не исклучиво безбедносните служби.

Најновата Стратегија за национална безбедност за периодот 2024–2029 година го квалификува странското мешање и манипулација со информации како еден од клучните предизвици за националниот суверенитет и за стабилноста на демократските процеси, интегрирајќи го овој феномен во поширокота проценка на безбедносното опкружување. Во деловите посветени на шпионажата и активностите на странските разузнавачки служби (II.1.7), ваквите дејствија се концептуализираат како реална, структурна и сериозна закана. Тие се третираат како составен елемент на поширок хибриден пристап насочен кон влијание врз внатрешната стабилност преку поттикнување политичка конфронтација, продлабочување на меѓуетничката и/или верската поларизација, како и систематско промовирање евроскептични наративи со цел ерозија на довербата во НАТО и евроатлантската интеграција. Особено внимание се посветува на таргетирањето организации, политички актери и поединци поврзани со екстремистички идеологии, кои можат да функционираат како посреднички канали за обликување на јавното мислење.

Хибридните закани дополнително се идентификувани како еден од најбрзо растечките безбедносни предизвици на регионално и на глобално ниво. Стратегијата забележува дека ваквите закани се реализираат преку синхронизирани и координирани активности што потекнуваат од државни, но и од недржавни актери. Во нивната реализација често се користи широка мрежа на посреднички структури, вклучително невладини организации, политички субјекти, религиозни групи и јавни личности, што ја усложнува нивната идентификација и институционалниот одговор.

Аналитичката проценка во Стратегијата потенцира дека овие операции имаат за цел долгорочно влијание врз стратегиската ориентација на државата и врз општествената кохезија. Клучните методи што се идентификуваат опфаќаат политичка субверзија, економски притисок и операции со информации, вклучително финансирање и инструментализација на медиуми, систематско ширење дезинформации и злоупотреба на дигиталните платформи и онлајн пор-

талите. Стратегиската намера на овие активности се поврзува со зголемување на социјалните поделби, поттикнување етнички национализам, создавање атмосфера на јавна вознемиреност и поткопување на довербата во демократските институции (II.1.8).

Стратегијата експлицитно се осврнува и на странското злонамерно влијание (II.1.9), при што именува конкретни државни актери и нивните стратегиски насоки. Во македонскиот контекст се нагласува дека руското влијание се манифестира преку мешање во демократските процеси, масовни кампањи за дезинформирање, злонамерни киберактивности и нелегални разузнавачки операции. Дополнително, се посочува употребата на домашни посредници – политички партии, актери од граѓанското општество и медиуми – како механизам за забавување или за поткопување на евроатлантската интеграција и влијание врз стратегискиот избор на земјата.

Во рамките на политичките цели поврзани со заштитата на националната безбедност, Стратегијата го дефинира Советот за координација на безбедносно-разузнавачката заедница како централно тело задолжено за обезбедување стратегиски насоки, усвојување заклучоци и предлагање мерки за справување со хибридни закани (III.1.4). Неговата функција опфаќа и надзор над имплементацијата на националната Стратегија за отпорност и на придружниот Акциски план, во согласност со стандардите на НАТО и ЕУ.

Дополнително, во рамките на политичката цел III.4.2 („Спротивставување на дезинформациите и развивање на медиумската писменост“), Стратегијата ја позиционира борбата против дезинформациите како суштински елемент на поширокиот одговор кон хибридните закани. Особено значајна е одредбата за воспоставување централно координативно тело составено од институционални комуникатори од клучните сектори – Владата, одбраната, надворешните работи, внатрешните работи, образованието, здравството и други релевантни области. Ова тело би имало мандат да ги координира институционалните активности поврзани со дезинформациите и да поддржува кохерентен национален пристап кон справувањето со странското мешање и манипулација третирајќи ја дезинформацијата како еден од нејзините централни оперативни аспекти.

Партнерството за безбедност и одбрана меѓу ЕУ и Македонија креира јасна иницијатива за усогласување

Значаен развој со директна стратегиска релевантност претставува воспоставувањето на Партнерството за безбедност и одбрана помеѓу ЕУ и С Македонија, кое опфаќа области на соработка што имаат непосредна поврзаност со информациските закани, градењето отпорност и стратегиската комуникација. Ова Партнерство дополнително ја зацврстува потребата од усогласување на националните институционални практики со пристапите, терминологијата и координативните стандарди што се развиваат во рамките на ЕУ.

Во таа смисла, документот придонесува кон институционална компатибилност со очекувањата на европските партнери и ја олеснува идната соработка преку примена на аналитичка и оперативна логика што сè повеќе се афирмира во рамките на ЕУ. Ова подразбира користење заеднички концептуални рамки, воспоставување повторливи процеси, како и систематско и документирано справување со инциденти поврзани со странско мешање и манипулација со информации.

2. Анализа на законските надлежности на клучните институции во Северна Македонија

Ефективноста на државниот одговор кон странското мешање и манипулација со информации (СММИ) не зависи исклучиво од аналитичкиот капацитет и степенот на свеста за ситуацијата, туку и од јасно дефинираните институционални мандати и надлежности што го овозможуваат нивното практично операционализирање.

Овој дел нуди систематизиран преглед на надлежностите на клучните институции релевантни за откривање, проценка и одговор на операции поврзани со странско влијание. Неговата цел е да ги идентификува постојните правни основи што можат да послужат како темел за воспоставување институционален модел насочен кон координирано управување со инциденти поврзани со странско мешање и манипулација со информации.

2.1. Агенција за разузнавање

Агенцијата за разузнавање располага со законски мандат за прибирање и обработка на разузнавачки информации поврзани со закани што потекнуваат од странство, со цел заштита на националната безбедност и стратегиските интереси на државата. Иако релевантната законска рамка експлицитно не го артикулира концептот на странско мешање и манипулација со информации, категоријата „закани и ризици од странски извори“ обезбедува функционална правна основа за институционален ангажман во случаи на координирани активности што подразбираат странско влијание.

Кампањите за манипулација со информации често се карактеризираат со инфраструктура која функционира надвор од националните граници, со надворешна координација и со користење посреднички актери. Во овој контекст, мандатот на Агенцијата е релевантен за следење на екосистемите на странски закани и придонес кон разузнавачки проценки што го информираат процесот на донесување одлуки на национално ниво.

Сепак, самото прибирање разузнавачки информации не може да гарантира ефикасен институционален одговор доколку не е интегрирано во поширок механизам на координација што овозможува навремена институционална ескалација, систематско споделување информации и донесување оперативни одлуки.

2.2. Агенција за национална безбедност

Агенцијата за национална безбедност располага со широка надлежност насочена кон заштита на уставниот поредок, суверенитетот и основните права и слободи на државата.

Основана во 2019 година како дел од пошироките реформи на безбедносно-разузнавачкиот сектор, Агенцијата е позиционирана како централна национална безбедносна институција способна да функционира како клучен координативен јазол во контексти на хибридни закани. Во пракса, мандатот на Агенцијата овозможува нејзино ангажирање во комплексни инциденти поврзани со информации, кои истовремено допираат до сферата на националната безбедност,

јавната доверба и институционалната стабилност. Во рамките на националниот модел на одговор на странско мешање и манипулација со информации, Агенцијата често се идентификува како потенцијална фокусна точка за рано предупредување, институционално алармирање и меѓусекторска координација. Ваквата улога не ја позиционира како единствен носител на одговорноста, туку како институција способна да интегрира влезни информации од повеќе области.

2.3. Министерство за одбрана и Закон за одбрана

Иако Законот за одбрана експлицитно не го третира феноменот на странските мешања и манипулации со информации, тој сепак содржи релевантни одредби поврзани со разузнавачките и контраразузнавачките активности, како и со спречување на странски субверзивни дејствија насочени кон одбранбениот сектор.

Кампањите за манипулирање со информации честопати вклучуваат наративи насочени кон поткопување на довербата во одбранбените институции, ослабување на кохезијата на алијансата и влијание врз процесите на донесување одлуки поврзани со безбедноста. Оттука, секторот одбрана има значајна улога во одредени категории инциденти, особено оние што се поврзани со НАТО, воената легитимност или стратегиски безбедносни кризи.

Сепак, мандатот на Министерството за одбрана останува првенствено секторски ориентиран. Иако неговата улога е од суштинско значење за одредени видови инциденти, тој не може да функционира како единствен институционален носител на националниот одговор кон странското мешање и манипулација со информации. Ефикасниот одговор бара воспоставување модел кој ќе значи координација на ниво на цела влада и цело општество.

3. Наоди од квалитативното истражување

Основната анализа беше дополнета со квалитативно истражување спроведено од Институтот за комуникациски студии (ИКС), кое беше спроведено преку полуструктурирани интервјуа со сегашни и поранешни високи јавни функционери, пратеници, комуникатори од институциите и јавни службеници, а беа направени и дополнителни експертски и стручни консултации со релевантни засегнати страни кои се вклучени во справувањето со странското мешање и манипулација со информации. Истражувачкиот тим стапи во комуникација со десет клучни државни институции кои беа избрани врз основа на нивните надлежности во делот на националната безбедност, надворешната политика и комуникацијата во услови на криза. Целта беше да се направи стратегиски пресек на безбедносната и политичката архитектура на државата, вклучувајќи ги сегашните и поранешните високи јавни функционери. Од десетте институции со кои беше контактирано, успешно беа спроведени шест длабински интервјуа. Овие учесници дадоа детални, „позадински“ увиди кои се потребни за да се разбере на кој начин моментално се обработуваат сигналите за манипулирање со информациите, да се идентификува каде се нарушува меѓуинституционалната координација и да се анализира зошто сегашните реакции и понатаму во голема мера се само по потреба.

Важно е да се појасни дека оваа методологија намерно става приоритет на капацитетите на државата и на владата. Европските рамки обично се залагаат за пристапот наречен „цело општество“, во кој се вклучени граѓанското општество, медиумите и технолошките платформи, додека ова истражување ја смета реакцијата од страна на „целата влада“ како темелен слој на националната отпорност.

Одлуката да се фокусираме на овие институционални перспективи, наместо на поширок примерок кој би се состоел од повеќе засегнати страни беше поттикната од потребата да се процени институционалната основа на државата. Воспоставувањето јасни внатрешни стратешки оперативни процедури, задачи и координативни тела претставува функционален предуслов: сè додека „оние кои први реагираат“ во државата не бидат синхронизирани, поширокаta општествена мобилизација и понатаму ќе биде недоволно изградена. Поради тоа, овие интервјуа се повеќе како специјализирана проценка на суверената одговорност на државата да го брани демократскиот информациски простор.

Целта на ова истражување беше да се утврди дали институциите во Македонија располагаат со практични протоколи и координирани процедури за управување со инциденти поврзани со странско мешање и манипулација со информации, надвор од формалното постоење на општи надлежности и стратегиското препознавање на хибридни закани.

Наодите укажуваат дека, иако свеста за заканата е на повисоко ниво, институционалниот одговор останува во голема мера фрагментиран и недоволно формализиран.

Откривањето на странско мешање и манипулација со информации е првенствено поврзано со секторот за безбедност и разузнавање

Конзистентен наод што произлегува од спроведените интервјуа е дека првичната идентификација на потенцијални инциденти поврзани со странско мешање и манипулација со информации најчесто се поврзува со безбедносно-разузнавачкиот сектор.

Испитаниците нагласуваат дека операциите на странско влијание и понатаму доминантно се перципираат првенствено низ призма на националната безбедност, особено во ситуации кога се инволвирани сомнителни надворешни актери, геополитички цели или координирани кампањи за манипулација.

Како последица на ваквата перцепција, како примарни точки на алармирање и проценка на ризик најчесто се посочуваат институции како што се Агенција за национална безбедност или Агенцијата за разузнавање, наместо цивилни министерства или сектори за комуникација.

Оваа практика рефлектира поширока институционална логика според која странското мешање и манипулација со информации се третира како специјализирана безбедносна проблематика, а не како оперативен предизвик што бара координиран пристап на ниво на владата.

Координацијата и понатаму е ад хок и зависи од неформална институционална иницијатива

И покрај постоењето на релевантни институции и потенцијални координативни структури, истражувањето потврдува дека во Македонија сè уште недостасува усогласен и формализиран модел за меѓуинституционален одговор на инциденти поврзани со странско мешање и манипулација со информации. Ваквото институционално несогласување е поради постоењето на двоен недостаток кој доведува до јаз помеѓу разузнавањето и дејствувањето. Иако во рамките на безбедносниот сектор постојат специјализирани капацитети и техничка експертиза, она што исто така постои е изразено отсуство на наменски координативни структури во рамките на министерствата.

Дополнително на горенаведеното, ваквата состојба е уште повеќе усложнета со системското отсуство на оперативни процедури во постојните рамки. Без ваквите интерни „упатства“, дури и институциите кои имаат соодветен законски мандат не се во можност да го преведат стратешкото препознавање во предвидлив и синхронизиран одговор. Сето ова прави државата да биде зависна од индивидуална иницијатива и неформални мрежи, наместо од институционализирана отпорност,

што значително ја попречува можноста за воспоставување обединета одбрана од софистицирани информациски закани.

Наместо тоа, одговорите имаат тенденција да се појават преку:

- неформални комуникациски канали,
- институционална проценка која се прави од случај до случај, и
- реактивно ангажирање базирано на индивидуална иницијатива.

Ваквата практика создава систем во кој институционалното дејствување не се темели на однапред дефинирани оперативни протоколи, туку на импровизација во однос на ситуацијата. Отсуството на јасни оперативни патеки значи дека слични инциденти можат да бидат третирани различно во зависност од тоа која институција е вклучена, од персоналниот состав на раководните структури или од перципираната политичка чувствителност на конкретниот случај.

Недостаток на јасно дефинирани улоги, одговорности и процедури за ескалација

Испитаниците конзистентно истакнуваат дека институционалните одговорности во контекст на странско мешање и манипулација со информации и понатаму не се доволно прецизно дефинирани.

Повеќе клучни процедурални аспекти остануваат без стандардизирани решенија, вклучително и определувањето на институцијата задолжена за прием на првиот сигнал, механизмите за почетна тријажа и приоритизација, критериумите за ескалација на инцидентот надвор од институцијата од која потекнува, протоколите за документирање и споделување на доказите, како и дефинирањето на водечкиот актер за јавната комуникација во случаи кога манипулацијата влијае на општествената доверба.

Во пракса, институциите претежно дејствуваат во рамките на своите законски надлежности, без постоење на интегриран оперативен механизам што би ги поврзал овие надлежности во еден кохерентен синџир на реагирање и одговор.

Ваквата состојба ја продлабочува институционалната фрагментација и го зголемува ризикот од задоцнети или недоследни реакции.

Ограничена свест кај институциите кои не припаѓаат на секторот безбедност

Иако свеста за заканите од манипулација со информации е релативно повисока во институциите кои се поврзани со безбедноста, испитаниците укажуваат дека во другите сектори на Владата и понатаму постои ограничено разбирање за странското мешање и манипулација со информации како системски и структурен ризик.

Во повеќе министерства и јавни тела, кампањите за манипулација сè уште се толкуваат во потесна смисла, и тоа како:

- медиумски дезинформации,
- изолирани случаи на дезинформација, или
- проблеми во комуникација, наместо координирани операции на влијание.

Овој јаз во институционалната перцепција ја ограничува способноста на граѓанските институции навремено да препознаваат рани сигнали, да проценуваат ризици и да придонесуваат за давање увид во сеопфатната ситуациска слика во државата.

Истовремено, ваквата нерамномерна подготвеност ја намалува ефикасноста на ниво на целата Влада, што е основен принцип во пристапите на EEAS и на Обединетото Кралство.

Отсуство на стандардизирана аналитичка методологија и прагови на ризик

Истражувањето укажува дека, иако институциите поседуваат одреден капацитет за неформална проценка на сериозноста на инцидентите поврзани со манипулација со информации, ваквите проценки ретко се темелат врз усогласени критериуми или врз структурирани аналитички рамки.

Нивоата на ризик најчесто се формулираат преку општи квалификации (ниско, средно или високо ниво на ризик), при што проценките остануваат претежно субјективни и недоволно методолошки утврдени.

Отсуството на заеднички аналитички стандарди ја ограничува можноста за:

- меѓусекторска споредливост на инцидентите,
- доследно приоритетизирање на ресурсите, и
- постепено градење на интероперабилно институционално знаење.

Во таа смисла, ваквата состојба дополнително ја нагласува потребата од примена на рамките како што се ABCDE и DISARM, кои овозможуваат заеднички аналитички јазик и алатки за класификација.

Потреба од централна координативна улога, во комбинација со дистрибуирана подготвеност на институциите

Испитаниците изразија голема поддршка за воспоставување на поцентрализиран механизам за координација, како алтернатива на постојната состојба во која кај повеќе институции може да има преклопување или нејасни надлежности.

Во тој контекст, Агенцијата за национална безбедност често беше посочувана како институција која располага со најсоодветни предуслови за да биде централен јазол за тревожење и координација, поради нејзината законска надлежност и меѓусекторска релевантност.

Притоа, испитаниците нагласуваат дека централната координација не подразбира дека одговорноста треба да биде исклучиво кај една институција. Напротив, ефективниот одговор бара постоење на споделена институционална одговорност, структурирана соработка помеѓу секторите и јасно дефинирани комуникациски улоги кај цивилните тела.

Токму тука стануваат оперативно значајни аналитичките рамки кои беа презентирани претходно во овој документ. ABCDE рамката поддржува структурирано разбирање на инцидентите, DISARM овозможува класификација на непријателските техники, а циклусот на анализа според EEAS обезбедува модел за повторувачки институционални процеси. Сите заедно, овие алатки можат да се преточат во стандардни оперативни процедури на национално ниво, јасни механизми за ескалација и структурирани шаблони за одговор во случај на инциденти.

Меѓународната пракса, вклучително и циклусот на анализа на EEAS и моделот RESIST на Обединетото Кралство, истакнува дека за да има успешен одговор, потребно е следново:

- заедничка слика за ситуацијата кај институциите,
- јасни механизми за ескалација,
- дефинирани улоги за анализа и комуникација, и
- стандардизирани процедури за споделување информации и документација.

Во отсуство на овие елементи, институционалните реакции остануваат ад хок, зависни од неформални мрежи и подложни на доцнење или на дуплирање.

Резиме на констатациите за Македонија

Квалитативното истражување потврдува неколку основни заклучоци:

- Македонија има воспоставено основни законски надлежности и стратегиски ги препознава заканите поврзани со странско мешање и манипулирање со информации.
- Сепак, институционалниот одговор е фрагментиран, неформален и недоволно операционализиран.
- Во моментов недостасуваат јасни стандардни оперативни процедури и механизми за ескалација како заеднички аналитички стандарди.
- Свеста и капацитетот се на различно ниво кај различни сектори од Владата.
- Координираниот модел на национално ниво бара постоење на централно лидерство и подготвеност на ниво на целата Влада.

Овие констатации ја даваат основата за развој на оперативните резултати од TRACE, кои имаат за цел да ја претворат постојната институционална инфраструктура во практични и повторувачки процедури за справување со инциденти и координација.

4. Европска Унија: Градење заедничка рамка за борба против странско мешање и манипулација со информации

Справувањето со странското мешање и манипулација со информации во Европската Унија претставува утврден и сè поизразен стратегиски приоритет. Ова произлегува од транснационалниот карактер на современите операции на влијание, кои по својата природа не се ограничуваат со државните граници, туку се шират низ повеќе држави, дигитални платформи и институционални екосистеми, а се осмислени постепено да ги искористуваат слабостите во демократските системи.

Во овој контекст, ЕУ во последниве години систематски развива заеднички пристап со разбирање, анализа и одговор на странско мешање и манипулација со информации. Иако овој пристап и понатаму е во еволуција, неговата насока е јасно дефинирана: институциите не можат да се потпираат исклучиво на реактивни механизми како проверка на факти или на демантирање на поединечни неточни приказни. Наместо тоа, неопходни се аналитички и оперативни алатки што овозможуваат препознавање координирани операции, атрибуција на актерите, анализа на употребените тактики и проценка на потенцијалното системско влијание.

Централна улога во овој процес има Европската служба за надворешни активности (EEAS), воспоставена во 2011 година како сервис за дипломатска и надворешнополитичка служба на ЕУ. Со текот на времето, EEAS се позиционира како водечка институција во координацијата на

европскиот одговор кон странското мешање и манипулација со информации. Нејзините активности опфаќаат следење на кампањи за влијание, анализа на модели на манипулација, поддршка на меѓуинституционалната координација и придонес кон градењето отпорност против информациските закани. Во рамките на оваа служба функционираат и работни групи за стратегиска комуникација, кои соработуваат со партнери во различни региони, вклучително и Западен Балкан, со цел зајакнување на отпорноста кон надворешни манипулативни наративи и поддршка на комуникациjата со ЕУ[4]. Нивната улога не се ограничува само на пренесување на официјални пораки на ЕУ туку опфаќа и систематска анализа на непријателските кампањи и механизмите преку кои тие влијаат врз јавната сфера.

Клучна карактеристика на современиот европски пристап е концептуализацијата на странското мешање и манипулација со информации како долгорочен, координиран и намерен модел на однесување, а не како збир на изолирани дезинформациски инциденти. Операциите на влијание најчесто се реализираат преку мултиканални стратегии, насочени кон специфични целни групи, со репетитивна употреба на одредени наративи и со цел создавање кумулативни ефекти – како ерозија на довербата во институциите, продлабочување на општествената поларизација или влијание врз политичкото одлучување.

EEAS го дефинира странското мешање и манипулација со информации како „претежно нелегален модел на однесување што се заканува или има потенцијал негативно да влијае врз вредностите, процедурите и политичките процеси. Таквата активност е манипулативна по својот карактер и се спроведува намерно и на координиран начин од страна на државни или други актери, вклучувајќи ги и нивните претставници во и надвор од нивната територија“.[5] Овие активности се намерни, координирани и можат да ги спроведуваат државни или недржавни актери, како и од нивните претставници, и во рамките и надвор од територијата на државата која е цел на активностите.

Со оглед на релативната новина и динамиката на оваа област, аналитичките алатки и методологии на ЕУ во последните години забележаа значителен развој. Особено значаен е напорот за воспоставување заеднички аналитички јазик меѓу институциите и државите, со цел да се надмине фрагментацијата во терминологијата и методологијата. Без заеднички стандарди за дефинирање и класификација, соработката и размената на информации се значително отежнати.

Во таа насока, ЕУ користи повеќе комплементарни алатки и рамки, секоја со специфична функционална намена. Тие обезбедуваат структуриран систем за класификација на тактиките, техниките и процедурите што се применуваат во операциите за влијание, како и стандарден формат за документирање инциденти, со што се олеснува размената на наодите помеѓу институциите, државите и партнерите.

Како земја кандидат и близок партнер на ЕУ, Македонија се соочува со слични информациски притисоци и има потреба од методолошки пристапи што се институционално компатибилни. Разбирањето на овие рамки не претставува само аналитичка придобивка туку и предуслов за развој на национални стандардни оперативни процедури, јасни координативни канали и функционални механизми за институционален одговор, кои ќе одговараат на европските стандарди и ќе овозможуваат ефективна соработка со партнерите.

---

[4] European External Action Service (EEAS), EEAS Strategic Communication Task Forces. Достапно на: https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en

[5] European External Action Service (EEAS), 2025 EEAS Threat Report, March 2025, https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

Во таа смисла, продлабоченото разбирање на рамки како што се ABCDE, циклусот на анализа на EEAS, DISARM и матрицата на изложеност на странско мешање и манипулација со информации се од суштинско значење за проценка на нивната практична применливост во македонскиот институционален контекст. Нивната интеграција може да послужи како основа за креирање национални процедури за координација, стандардни оперативни процедури и алатки за одговор.

4.1. Аналитички основи за разбирање на странското мешање и манипулација со информации: ABCDE

Пред институциите да можат да воспостават ефективен одговор на странското мешање и манипулација со информации, неопходно е да поседуваат јасно концептуално разбирање на феноменот што го третираат. Во пракса, токму ова претставува еден од најзначајните предизвици. Значителен број субјекти сè уште го третираат странското мешање и манипулација како „лажни вести“ или како изолирани случаи на дезинформациски содржини. Меѓутоа, современите операции на влијание се суштински покомплексни: тие се карактеризираат со координирано дејствување, репетитивна употреба на наративи, постоење на мрежи за засилување на пораките и јасно дефинирана стратегиска намера.

Оттука произлегува потребата аналитичарите да располагаат со структуриран, но оперативно применлив модел за деконструкција на инцидентите поврзани со странско мешање и манипулирање со информации на нивните клучни составни компоненти.

Во таа насока, ABCDE-рамката[6] претставува една од најкорисните иницијални аналитички алатки. Таа е применувана во аналитичка практика на ЕУ, особено во процесот на структурирање на почетните проценки на координирани кампањи за влијание, вклучително и во извештаите на EEAS кои документираат манипулативни активности поврзани со актери наклонети кон Кремљ за време на значајни политички настани. Важно е да се нагласи дека ABCDE не претставува замена за сеопфатна истрага, туку обезбедува концептуална логика за утврдување дали конкретен инцидент може да се смета за дел од поширока операција на влијание.

Нејзината вредност се засилува при конзистентна примена во повеќе случаи, со што се овозможува идентификација на повторувачки обрасци, релевантни актери и типични методи на дејствување.

Рамката е изградена околу пет основни елементи:

Актер (A)

Првото прашање секогаш е: Кој стои зад активноста?

„Актер“ се однесува на потенцијалниот извор на заканата. Ова може да бидат странски државни актери, мрежи поврзани со разузнавање, организирани групи на посредници или координирани онлајн заедници. Во практиката, атрибуцијата претставува комплексен предизвик, со оглед на тоа што актерите на странското мешање и манипулација со информации често се скриени зад анонимни дигитални профили, посредници или зад лажно брендирање.

[6] European External Action Service (EEAS) (2023) EEAS Threat Report 2023. Достапно на: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

Притоа, од суштинско значење е аналитички да се разграничат актерите од каналите што се користат. Дури и во ситуации кога целосната атрибуција е ограничена, идентификувањето на веројатните типови актери им помага на институциите подобро да ја разберат мотивацијата, стратегиските цели и нивото на ризик.

Однесување (Б)

Вториот елемент се фокусира на тоа како дејствува актерот.

„Однесување“ ги опфаќа методите што се користат за влијание врз информациската средина, вклучително координирано неавтентично однесување, употреба на автоматизирани профили (ботови), мрежи на тролови, вештачко амплифицирање, кампањи за заплашување или манипулација со алгоритмите на платформата.

Овој аспект е од суштинско значење, бидејќи странското мешање и манипулација со информации се дефинираат не само според содржината туку и според моделите на координирано однесување. Индикациите кои го покажуваат однесувањето често даваат посилни докази, отколку самата сличност на наративот.

Во овој контекст, рамките како DISARM, кои се образложени понатаму во текстот, имаат особена аналитичка вредност, бидејќи придонесуваат за методолошка конзистентност.

Содржина (В)

Третиот елемент е самата порака.

„Содржина“ се однесува на наративите, форматите и типовите информации што се користат во операцијата. Тоа може да вклучува целосно измислени приказни, манипулирани медиуми, ставање во погрешна рамка, селективна употреба на факти или емоционално набиени пораки кои имаат за цел да предизвикаат страв, лутина или недоверба.

Анализата на содржината овозможува институциите да препознаат со каков вид информациска закана се справуваат, без разлика дали станува збор за дезинформации, погрешни информации или злонамерни информации, и дали е тоа поврзано со наративи за влијание кои се претходно познати или со нови теми.

Степен (Г)

Четвртиот елемент се занимава со обемот и ширењето на содржината.

„Степен“ се однесува на тоа колку широко циркулира содржината и колку јако се засилува. Ова значи големина на публиката до која допрела информацијата, брзината на нејзино ширење, платформите кои се користат и присуството на координирани механизми за поттикнување (boosting).

Овој аспект е клучен за процесот на приоритетизација на институционалниот одговор. Не секој инцидент бара исто ниво на одговор. Разбирањето на степенот на изложеност им помага на институциите да разграничат дали проблемот е само маргинален настан или е дел од поголема кампања.

Овој вид проценка се поддржува со аналитички алатки како Матрицата на изложеност на странско мешање и манипулација со информации, развиена од EEAS, и тоа преку мапирање на каналите и нивоата на поврзаност со непријателски актери.

Ефект (E)

Последниот елемент се фокусира на влијанието.

„Ефект“ се однесува на исходот што операцијата настојува да го постигне и на влијанието што го има врз целната средина. Во многу случаи, целта не е да се убедат луѓето во некое лажно тврдење, туку постепена ерозија на довербата, создавање конфузија, делегитимирање на институциите, обесхрабрување на учеството или интензивирање на општествената поларизација.

Систематската анализа на ефектите им овозможува на институциите да проценат колку е опасна конкретната операција и каков вид одговор е пропорционален и неопходен.

Во овој контекст, рамката ABCDE има особена институционална вредност, бидејќи воспоставува заеднички јазик. Таа им овозможува на различни актери, од безбедносни служби до владини комуникатори, да го опишат истиот инцидент со користење категории кои можат да се споредуваат.

4.2. Циклус на анализа

Рамката ABCDE им помага на институциите систематски да ја деконструираат структурата на инцидентот со странско мешање и манипулирање со информации: кој стои зад него, како функционира, каква содржина се користи, колку далеку се шират тие информации и каков ефект имаат цел да постигнат. Сепак, на институциите им е потребен и јасно дефиниран оперативен процес за насоката на нивното постапување откако ќе се открие таквиот инцидент.

Во таа насока, Европската служба за надворешни активности (EEAS) го разви циклусот на анализа,[7] кој, за разлика од рамката ABCDE која гледа на работите низ концепциска смисла, е оперативен работен тек. Тој објаснува како институциите треба да следат, да даваат приоритет, да истражуваат, да документираат и да споделуваат информации за инциденти поврзани со странско мешање и манипулирање со информации, и тоа на структуриран и репетитивен начин.

Целта на циклусот е надминување на ад хок реагирањата и воспоставување конзистентен институционален процес што со текот на времето акумулира знаење. Тој обезбедува основа за координирана анализа и одговор, што е од суштинско значење за развој на стандардни оперативни процедури и процедури за справување со инциденти на национално ниво. Циклусот на анализа на EEAS чекор по чекор го претвора она што се знае за странското мешање и манипулирање со информации во практичен процес. Рамката ABCDE помага да се опише некој инцидент, а циклусот на анализа објаснува како институциите треба да работат во однос на тој инцидент на организиран начин – од рано откривање до долгорочна свесност за ситуацијата.

Циклусот се состои од пет последователни фази:

Фаза 1: Стратегиски мониторинг

Оваа фаза вклучува континуирано и организирано следење на познати канали, актери и инфраструктури што се користат за манипулација со странски информации. Ова подразбира веб-страници, профили на социјалните медиуми, медиуми и други платформи кои претходно биле поврзани со активност на влијание. Целта е рано откривање на сигналите пред тие да ескалираат.

[7] Европска служба за надворешни активности (EEAS), Извештај за заканите на EEAS за 2023 година, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

Фаза 2: Приоритизирање и тријажа

Не секоја сомнителна порака бара исто ниво на внимание. Оваа фаза служи како филтер и им помага на институциите да ги насочат ресурсите кон оние случаи кои се од посериозна природа, кои се покоординирани или имаат поголем потенцијал да предизвикаат штета. Таа ги одделува маргиналните појави од инцидентите со повисок ризик.

Фаза 3: Анализа на инциденти и собирање докази

Ова е централната аналитичка фаза во која аналитичарите прават потемелно истражување со користење отворени извори и достапни податоци. Тие истражуваат како се шири содржината, каде првпат се појавила, кои мрежи ја засилуваат и какви тактики, техники и процедури се користат. Тука се особено важни структурираните алатки како што е DISARM.

Фаза 4: Споделување на знаење и координација

Анализата е корисна само ако успее да допре до актерите кои можат соодветно да одговорат. Во оваа фаза, наодите се споделуваат со релевантните засегнати страни и со партнерите. На подолг рок, инцидентите се документираат со користење стандардизирани формати, така што можат да се споредат, да се складираат и да се користат за идно учење.

Фаза 5: Свесност за ситуацијата

Последната фаза се фокусира на градење подлабоко разбирање на заканите. Со текот на времето, повторувањето на циклусот им помага на институциите да препознаат обрасци, нови актери и тактики кои постојано се менуваат. Мониторингот се проширува врз основа на нови наоди, а институционалниот одговор станува подобро информиран и проактивен.

4.3. Рамка DISARM

Откако институциите ќе бидат во можност да препознаат инцидент со странско мешање и манипулација со информации и да следат основен процес на анализа, следен предизвик е како да се опише, на прецизен и споредлив начин, што, всушност прави, непријателскиот актер?

За разлика од ABCDE, кој помага да се објасни целокупната структура на инцидентот, и за разлика од циклусот на анализа, кој го објаснува работниот тек на институционалната анализа, DISARM[8] се фокусира на оперативното однесување на актерот кој претставува закана.

DISARM (Анализа на дезинформации и управување со ризици) е рамка со отворен код која е развиена од Фондацијата DISARM и која широко се користи од аналитичарите на странското мешање и манипулација со информации во ЕУ, од структурите поврзани со НАТО и од земјите-партнери. Нејзина цел е да обезбеди заедничка таксономија, што значи заеднички јазик за документирање и класифицирање на тактиките и техниките што се користат во манипулативните кампањи.

Операциите на странско мешање и манипулација со информации ретко се изолиран настан.

[8] DisARM Foundation, DisARM Navigator. Достапно на: https://disarmfoundation.github.io/disarm-navigator/

Истиот актер често повторува слични методи во разни земји, на различни платформи и во различни временски периоди. Доколку не постои стандарден начин за опишување на овие методи, институциите не можат лесно да споделуваат констатации, да споредуваат случаи ниту, пак, да градат системи за рано предупредување. DISARM е создаден од идејата да се создаде „синџир кој ќе ги убива дезинформациите“, што значи дека кампањите за манипулација следат логичен редослед на чекори – од планирање до извршување и проценка. Рамката ги организира овие чекори во фази, и во рамките на секоја фаза идентификува конкретни тактики и техники.

Четирите главни фази на DISARM се следниве:

Планирање: Актерот ја дефинира стратегиската цел на операцијата, избира целна публика и го осмислува планираниот резултат.

Подготовка: Актерот ја гради инфраструктурата потребна за спроведување на кампањата, како што се лажни профили, посреднички медиуми, координирани мрежи и прилагодени наративи.

Извршување: Кампањата се започнува преку дистрибуција на содржина, засилување, координација помеѓу платформите, а понекогаш и преку мобилизација надвор од интернетот.

Оценување: Актерот ги мери ефектите, ги приспособува пораките и одлучува дали да ескалира, да ги повтори или да ги промени тактиките.

Клучната вредност на DISARM е тоа што им овозможува на институциите да препознаат модели на однесување, а не само индивидуални лажни тврдења. Следејќи ги тактиките и техниките кои се користат, аналитичарите можат да го препознаат „потписот“ на актерот кој има непријателска намера и да интервенираат рано во текот на неговата операција, пред истата да создаде поширок општествени ефекти.

4.4. Матрицата на изложеност на странско мешање и манипулација со информации

Откако DISARM им помогна на институциите да разберат што прават актерите со непријателска намера, следното прашање е преку кои канали се реализира влијанието?

Операциите на странско мешање и манипулација со информации се шират преку слоевити мрежи на профили, веб-страници, инфлуенсери, посреднички медиуми и преку координирано засилување на пораките. Во таков контекст, идентификувањето на целосната инфраструктура на влијание често е многу поважно отколку фокусирањето само на оригиналната порака.

За да го поддржи ваквиот вид структурирано мапирање, Европската служба за надворешна акција (EEAS) ја разви Матрицата за изложеност на странско мешање и манипулација со информации во својот Трет извештај на EEAS.

За разлика од ABCDE, која го расчленува инцидентот, и за разлика од DISARM, која ги класифицира тактиките и техниките, Матрицата на изложеност се фокусира на припишување и изложување. Нејзината улога е да им помогне на аналитичарите и институциите да категоризираат различни извори врз основа на тоа колку директно се поврзани со непријателски актер. Таа обезбедува јасна терминологија со која се опишуваат овие канали и нивното ниво на поврзаност со странскиот актер. Ова им олеснува на институциите да создаваат одговори кои се засновани на докази и ефикасно да се координираат со партнерите при разоткривање на странско мешање и манипулација со информации и справување со него.

Оваа аналитичка алатка е од суштинско значење бидејќи во голем број случаи каналите кои имаат најголемо влијание не се отворено поврзани со странска држава. Наместо тоа, тие функционираат преку индиректни или скриени врски, што го отежнува одговорот од институциите.

Матрицата има четири главни цели. Прво, таа е поддршка во мапирањето на инфраструктурата. Им помага на аналитичарите да видат подалеку од најочигледните извори и да ја земат предвид поширокатa мрежа со која се засилува манипулацијата. Второ, го зајакнува припишувањето базирано на докази. Матрицата ги охрабрува институциите да се потпираат на техничките индикатори и на индикаторите на однесување, а не само на сличноста на наративот, намалувајќи го на тој начин ризикот од прекумерно припишување. Трето, таа поддржува анализа со користење на повеќе извори. Ефективната проценка бара комбинирање на информации кои потекнуваат од отворен извор со податоци кои се од институции, од комерцијална природа или потекнуваат од партнери. Четврто, таа го подобрува пропорционалниот одговор. Имањето разбирање за тоа каков вид на канал се користи, институциите можат да применат целни контрамерки и да избегнат непотребна ескалација.

Матрицата на изложеност се заснова на две клучни оски.

Првата оска е 'припишано' наспроти 'неприпишано'. Каналите на кои им се припишува дејствување се оние каде што постојат силни докази кои директно ги поврзуваат со државен актер. Каналите на кои не им се припишува дејствување се канали кои покажуваат усогласеност или координација, но не постојат доволно докази за формална атрибуција.

Втората оска е 'отворена' наспроти 'прикриена'. Отворените канали отворено ја кажуваат својата афилијација кон државата. Прикриените канали ги кријат своето потекло, сопственост или координација, и работат преку посредници или прикриени мрежи.

Со комбинирање на овие оски, институциите можат да ги класифицираат каналите на влијание во конкретни категории кои се одраз на различни нивоа на изложеност и одговорност.

5. RESIST 3: Пристапот на Обединетото Кралство во борбата против странско мешање и манипулација со информации

Ако пристапот на ЕУ во голема мера се однесува на градење заеднички аналитички јазик (како јасно и доследно да се опише странското мешање и манипулација со информации), моделот на Обединетото Кралство UK RESIST се однесува на тоа што институциите, всушност, треба да прават кога манипулацијата ќе почне да се шири.

RESIST 3[9] е структурирана рамка наменета за комуникатори во институциите на државата.

[9] Department for Science, Innovation and Technology (DSIT) (2025) RESIST 3: A Framework for Building Government Communication Resilience. Достапно на: https://www.communications.gov.uk/wp-content/uploads/2025/10/RESIST-FINAL.pdf

Развиена е од д-р Џејмс Памент (James Pamment – кој придонеел и кон ABCDE) и се користи како практичен пристап за градење отпорност против информациски закани. Не е рамка за разузнавање, ниту, пак, е воена доктрина. Поблиску е до институционален „прирачник“ наменет за комуникатори од јавниот сектор, за прес-службите и за лицата што носат одлуки, а кои треба да реагираат брзо, но одговорно. RESIST сега е во својата трета верзија, бидејќи Обединетото Кралство во меѓувреме направи ажурирање на моделот, и тоа врз основа на реално искуство со кампањи за дезинформации и промени во информациската средина. Првите верзии се фокусираа главно на основен комуникациски одговор. Третата верзија е најразвиена и најпрактична, бидејќи вклучува упатства за градење долгорочна институционална отпорност и реагирање на поструктуриран начин, вклучително и во контекст на нови технологии како што е вештачката интелигенција.

Дополнително, таа предлага реални комуникациски канали, оперативен тек и образец за одговор на инциденти што може да функционира кај министерствата и кај институциите. RESIST е еден од најдобрите меѓународни примери за тоа како аспектите поврзани со странско мешање и манипулација со информации да се преточат во секојдневна институционална пракса.

Од наведените причини, RESIST 3 има особена релевантност за македонскиот институционален контекст. Поголемиот дел од институциите во државата не се разузнавачки агенции, туку министерства, јавни комуникатори и официјални лица на кои им се потребни јасни и едноставни процедури во случаи кога манипулациите се шират на интернет. RESIST 3 го овозможува токму тоа.

Пристапот кој го користи RESIST не се ограничува само на „борба против дезинформации“ туку и зајакнување на довербата и намалување на ранливоста. Тој исто така ги зема предвид и поновите технологии, како што е вештачката интелигенција, и го подобрува начинот на кој институциите прават проценка на заканите и ранливоста. Ова е клучен аспект кога зборуваме за оваа проценка, бидејќи еден од постојано присутните проблеми е тоа што проценките на ризикот често се неформални, недоследни и не се споделуваат со други.

Во јадрото на RESIST е концептот на отпорност (resilience), кој во овој контекст подразбира способност на институциите да издржат напад со информации, приспособување за време на инцидентот и закрепнување по неговото завршување. Ова подразбира испраќање приспособени пораки, подготовка, координација, градење доверба и учење од минати инциденти.

Дополнително, RESIST подразбира пристап на ниво на целото општество. Владата не може и не треба да го понесе целиот товар, туку во соработка со други институции, медиуми, граѓанското општество и доверливи општествени актери како интегрален дел од стратегијата.

Во оваа смисла, RESIST експлицитно нагласува дека комуникацијата на ниво на влада е суштинската прва линија на одбрана кога се работи за странско мешање и манипулација со информации. Ако институциите комуницираат лошо, доцна или недоследно, тие создаваат простор за зголемување на манипулацијата.

5.1. Шесте чекори на RESIST 3

RESIST е структуриран во шест меѓусебно поврзани чекори. Целта е тие да се користат како циклус кој се повторува, а не како еднократна листа (checklist). Институциите можат да влезат во циклусот во разни фази во зависност од ситуацијата, но логиката останува иста: рано откривање, разбирање што се случува, проценка дали е потребна интервенција, пропорционален одговор и учење од она што се случило.

Препознавање

Главната цел на „Препознавање“ е да се обезбеди дека сите владини комуникатори имаат основно разбирање на тоа каква е механиката на дезинформациите, погрешните информации и злонамерните информации, природата на нивното засилување преку алгоритми и за стратешките цели на непријателските актери. Доколку „Препознавање“ се третира како столб на професионален развој, а не како активатор за реактивно постапување, институциите ќе можат да изградат поотпорна и поинформирана фронтовска линија против мешање во информациите. Ваквата основна едукативна програма во мирновременски услови гарантира дека комуникаторите ќе бидат способни за рано идентификување (се работи за суштинската фаза „забележи го пред да се прошири“) што им овозможува да откриваат сомнителни наративи или синтетичка содржина без претходно да бараат целосна проценка преку разузнавање.

Во оваа фаза од особена важност се основните индикатори. RESIST ја промовира употребата на структурирани промптови, како што е FIRST (фабрикување, идентитет, реторика, симболизам, технологија). Поентата не е дека секој комуникатор треба да стане аналитичар, туку да се обезбеди јасна рамка преку која евентуалниот инцидент може аргументирано да се пријави и да се образложи, со што ќе се намали можноста за произволна проценка.

Во однос на претходно разгледаните рамки, овој чекор директно е поврзан со ABCDE и со циклусот на анализа. Препознавањето претставува почетна точка на институционалната тријажа. Доколку овој чекор е слаб, целиот последователен процес станува реактивен.

Рано предупредување

Наместо да следат сè, институциите треба да воспостават јасна рамка за приоритизација на ризиците. Тоа подразбира идентификација на чувствителните области, како што се избори во државата, безбедносни кризи, етнички тензии, одлуки во врска со надворешната политика или големи инциденти, како и идентификација на целните публики што се најзагрозени или најважни во тој контекст.

Раното предупредување станува функционално само кога институциите имаат јасно дефинирани задачи за следење и прецизни правила за ескалација на случувањата. Тоа не претставува исклучиво техничка способност туку и прашање за институционалната дисциплина: кој што гледа, кој известува и колку брзо.

Во однос на претходно разгледаните аналитички рамки, овој чекор е директно поврзан со првите две фази од циклусот на анализа (стратегиско следење и приоритизација/тријажа), но пренесено во институционален контекст.

Увид во ситуацијата

Увидот во ситуацијата значи сумирање на релевантните информации во форма што е кратка, прецизна и оперативно употреблива. Не станува збор за обемен извештај, ниту за соопштение за медиумите, туку за краток извештај што дава јасен одговор за клучните прашања: што се случува, кој стои зад тоа (доколку е познато), кој е таргетиран, како се шири и што би можело следно да се случи.

Овој чекор има критична важност во македонски контекст. Досегашните проценки укажуваат дека институциите често не располагаат со заедничка, усогласена претстава за ситуацијата. Дури и кога поединци навремено детектираат проблем, сознанијата за тоа што се случува остануваат во

рамките на една канцеларија или во една институција. Увидот во ситуацијата е мостот помеѓу „некој забележал нешто“ и „системот реагира“.

Анализа на влијанието

Овој чекор се однесува на тоа дали е потребна институционална интервенција и доколку е така, со каков интензитет да биде. RESIST не сугерира дека државата треба да биде таа која ќе каже што е вистината во секој од случаите. Наместо тоа, клучното прашање е: каква е веројатната штета што може да произлезе од конкретниот случај?

Анализата на влијанието ги разгледува можните штети врз јавната безбедност, довербата во институциите, демократските процеси, социјалната кохезија или спроведувањето на јавните политики. Воедно, таа го зема предвид и временскиот аспект: понекогаш истата нарација може да биде со мал ризик во еден момент, а со висок ризик во некој друг момент.

Практична карактеристика на овој чекор е идејата за прагови (thresholds). Институциите треба да дефинираат што значи „низок“, „среден“ и „висок“ ризик во пракса и какви видови одговори се соодветни за секое од овие нивоа.

Без ова, одговорот е политички, недоследен или задоцнет.

Стратегиска комуникација

Стратегиската комуникација може да вклучува низа мерки, во зависност од ризикот и видот на инцидентот.

Таа може да значи проактивна комуникација насочена кон превенција на веројатна манипулација, навремено појаснување на фактите кога се шират дезинформации, како и разоткривање на тактиките на манипулација кога постои доволна основа за припишување. Во одредени ситуации, стратегиската комуникација може да подразбира и ангажирање доверливи надворешни актери, наместо да се користи само гласот на Владата. Подеднакво важен е и аспектот на внатрешна координација, со цел да се обезбеди конзистентност и да се избегне контрадикторност меѓу институциите.

Основниот принцип е пропорционалноста, комбинирана со зачувување на кредибилитетот. Недоволен или задоцнет одговор може индиректно да ја засили манипулативната содржина, додека агресивниот одговор без докази може да создаде негативна реакција. RESIST ги насочува институциите кон интервенции што се одржливи на долг рок, наместо кон краткорочна „победа“.

Во однос на идната разработка на оперативниот тек, неопходно е јасно да се дефинираат институционалните улоги и одговорности: кој ги составува пораките, кој ги одобрува, кој координира меѓу институциите и како се балансираат брзината и точноста. Дополнително, рамката треба да вклучува и јасна артикулација на комуникациските цели, идентификација на целната публика, изборот на соодветните канали и проценката за нивото на ризик.

Ефективност на следење

Овој чекор претставува една од најчесто занемарувaните, но суштински компоненти на институционалниот одговор. Во отсуство на систематско следење на ефективноста, институциите ризикуваат да ги репродуцираат истите слабости, без акумулација на знаења.

Следењето на ефективноста подразбира двојна проценка: прво, дали конкретниот одговор бил соодветен, и второ, дали внатрешниот процес функционирал на начин што може да се смета за институционално одржлив.

Тоа вклучува прашања како: дали интервенцијата беше навремена, дали меѓуинституционалната координација беше ефикасна, дали штетата беше ограничена, дали беше избегната непотребна ескалација, дали пораките стигнаа до целната публика и дали беа извлечени применливи поуки за идни случаи?

Овој чекор не бара совршенство, туку воспоставување на едноставни, но конзистентни рутини: кратки прегледи по дејствувањето, документирање на лекциите и ажурирања на протоколите.

Кога одговорите се ад хок и учењето останува ад хок – фрагментирано, неформално и зависно од искуствата на ограничен број поединци. Спротивно на тоа, следењето на ефективноста овозможува трансформација на оперативното искуство во институционална меморија.

6. Следни чекори

Оваа проценка потврдува дека предизвикот во македонски контекст не се состои во отсуство на институции или во недостиг на законски надлежности за координиран одговор на странско мешање и манипулација со информации, туку во недостаток на усогласен и институционализиран начин на постапување кога ќе се појави конкретен инцидент. Анализата на интервјуата и релевантната литература овозможува идентификација на три структурни слабости. Прво, отсуствува јасно дефиниран и формално прифатен модел за координација што недвосмислено одговара на прашањата: кој ја презема водечката улога, кои институции обезбедуваат поддршка и во која фаза од процесот. Второ, не се воспоставени повторливи и предвидливи процедури за управување со инциденти кои би овозможиле систематски премин од иницијален сигнал кон аналитичка проценка, институционална одлука и јавна комуникација. Трето, институционалното разбирање на странското мешање и манипулација со информации останува нерамномерно, што резултира со различни интерпретации на идентичен инцидент – како комуникациски предизвик во една институција и како безбедносна закана во друга – што ја продлабочува фрагментацијата на одговорот.

Во овој контекст, разгледаните рамки нудат комплементарни решенија за различни сегменти од проблемот. ABCDE овозможува рана и структурирана деконструкција на инцидентот, насочувајќи го вниманието не само кон содржината туку и кон актерот, моделот на однесување, степенот на ширење и очекуваниот ефект. Циклусот на анализа на EEAS обезбедува оперативна логика преку која континуираниот мониторинг се трансформира во приоритетни случаи, детална истрага, систематско споделување на резултатите и долгорочна свесност за ситуацијата. DISARM ја стандардизира димензијата на однесување, овозможувајќи евидентирање и класификација на тактиките и техниките во унифициран формат – предуслов за препознавање шеми и за соработка со партнери. Матрицата на изложеност додава кон сето ова практичен модел за мапирање на канали и инфраструктура, што е важно во случаи кога кампањата користи комбинација од отворени извори, посреднички мрежи и скриено засилување на пораката.

Моделот RESIST на Обединетото Кралство има посебна применлива вредност за македонскиот институционален контекст, бидејќи е дизајниран токму за оние актери што најчесто се наоѓаат на првата линија на јавната комуникација за време на инциденти: владини комуникатори, прес-служби и тимови за политики кои мора да реагираат брзо, без импровизирање и без ескалација на паниката.

Овој модел обезбедува структурирана и повторлива рутина што ги води институциите низ клучните фази: препознавање на сигнали за манипулација, рано предупредување, овозможување увид во ситуацијата за носителите на одлуки, проценка дали е потребна интервенција врз основа на штетата, спроведување стратегиски комуникациски мерки, а потоа евалуација на ефективноста на одговорот. Доколку комуникаторите немаат основен прирачник, институционалните реакции имаат тенденција да станат ад хок, задоцнети, недоследни или сведени на комуникациска тишина.

Рамките на ЕУ овозможуваат институциите прецизно да ја дефинираат и да ја класифицираат заканата, користејќи терминологија заснована на докази, методолошка конзистентност и стандарди што ја олеснуваат соработката помеѓу партнерите. RESIST им помага на институциите да управуваат со инцидентот во реално време преку оперативна рутина што може да се примени во сите министерства. Со други зборови, рамките на ЕУ го градат „заедничкиот јазик“, а RESIST помага тој јазик да се претвори во институционално дејствување.

Врз основа на наодите наведени тука, се предлагаат следниве чекори со кои Северна Македонија ќе се придвижи од стратешка намера кон функционална операционализација:

- Напреден мониторинг на медиумите: Обука за алатки и техники за скенирање на информациската средина за појава на нови наративи.
- Идентификација и проценка на информациски закани: Развивање на способност за правење разлика помеѓу изворна домашна дебата и координирана манипулација (ОМИ/СММИ).
- Проценка на ризик и влијание: Воспоставување методологија за правење проценка на потенцијалот од тоа да се предизвикаат штети во јавноста, поделеност во општеството или од постоење безбедносни ризици кои би биле предизвикани од одредена кампања.
- Стратешки комуникации и евалуација: Совладување на уметноста на проактивно и реактивно испраќање пораки, проследено со ригорозна евалуација со цел да се утврди ефикасноста на интервенцијата.
- Етички стандарди и заштитни мерки за демократијата: Обезбедување секоја активност да се темели на транспарентност и точност и на принципот „Не нанесувај штета“.

- Протокол за Централното владино координативно тело: Во согласност со Националната стратегија за безбедност 2024 – 2029, овој чекор ќе го дефинира начинот на кој ќе функционира централно тело за синхронизирање на државните активности. Ова тело исто така ќе има улога и да биде основна врска помеѓу политичката комуникација и националната безбедност.
- Рамка за оперативен тек што треба да го дефинира институционалниот пат при инцидент со странско мешање и манипулирање со информации, почнувајќи од првичното негово откривање до заедничка проценка, ескалација, одлука, јавен одговор и преглед. Таа треба да разјасни кој кого свикува, кои канали се користат за итна координација, што е она што предизвикува ескалација и на кој начин информациите се споделуваат меѓу институциите без да има забуна или дуплирање.

- Шаблон за реагирање на инциденти кој треба да ја стандардизира документацијата, така што институциите нема да губат време дебатирајќи што треба да евидентираат и како. Тој треба да го опфати минимумот кој е потребен за давање поддршка во правењето анализа која е компатибилна со ЕУ и соработката на партнерите, како и јасна изјава за проценетото влијание и нивото на доверба. Стандардизираните шаблони се она што ги прави случаите споредливи, а тоа овозможува создавање институционална меморија и исто така овозможува научените лекции да се претворат во побрзи и подобри одлуки следниот пат.

Проширување во насока на рамка за отпорност која ќе го опфаќа „целото општество“

Станува збор за структуриран механизам за соработка помеѓу повеќе засегнати страни кој го премостува јазот кој постои помеѓу активностите на државата и надворешната стручна експертиза. Ваквиот резултат значи излегување од интерниот капацитет и искористување на потенцијалот на разните други актери кои се надвор од државниот апарат, и тоа преку:

- Партнерства помеѓу граѓанските и академските организации: Формализирање на начините преку кои граѓанските организации (ГО) и истражувачите обезбедуваат независен мониторинг, анализа на податоци и педагошка поддршка за иницијативите за медиумска писменост.
- „Црвен“ тим (или „Тим за тревога“) предводен од експерти: Ангажирање дигитални експерти, специјалисти за OSINT (Open-Source Intelligence specialists) и стручен кадар за кибербезбедност со цел симулирање на информациски напади и тестирање на постојните протоколи за одговор од страна на државата.
- Споделување информации меѓу јавниот и приватниот сектор: Воспоставување безбедни канали за комуникација во реално време со користење дигитални платформи и ангажирање технолошки експерти во насока на идентификување и ублажување на ширењето на странското мешање и манипулацијата со информации (СММИ) на самиот извор.
- Јавна свест: Развој на комуникациски кампањи во соработка со академски институции и граѓански организации со цел градење на граѓански „когнитивен имунитет“, со што се обезбедува дека на пораките кои се испраќаат може да им се верува, дека се инклузивни и дека допираат до маргинализираните заедници.
- Споделен репозитар на знаење: Креирање централизирана база на податоци до која ќе може слободно да се пристапува, во која ќе бидат содржани нови наративи и тактики, и која ќе биде достапна не само за владините комуникатори туку и за овластени партнери во истражувањето во насока на обезбедување заедничка слика во дејствувањето.

Оваа проценка покажува дека преку стратешките документи во Македонија сè повеќе се препознаваат хибридните закани, операциите преку информации и странското влијание како сериозни ризици. Тоа е усогласено со европската пракса и обезбедува поволно политичко опкружување. Слаба точка е оперативниот мост помеѓу стратегијата и секојдневниот одговор. Поради тоа, следната фаза треба да се фокусира на операционализација: земање на она што постои на хартија и овозможување тоа секогаш да функционира на ист начин, без оглед на тоа која институција прва го забележува сигналот.

6. Библиографија

1. DISARM Foundation, DISARM Navigator. Достапно на: https://disarmfoundation.github.io/disarm-navigator/
2. European External Action Service (EEAS), EEAS Strategic Communication Task Forces. Достапно на: https://www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en
3. European External Action Service (EEAS) (2023) EEAS Data Team Threat Report 2023 [PDF]. Достапно на: https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf
4. European External Action Service (EEAS) (2025) EEAS 3rd Threat Report (March 2025) [PDF]. Достапно на: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
5. NATO Strategic Communications Centre of Excellence (NATO StratCom COE) (2026) The NextGen Information Environment. Riga: NATO StratCom COE. ISBN 978-9934-619-76-2
6. Стратегија за градење национална отпорност и справување со хибридни закани [Strategy for building national resilience and addressing hybrid threats]. Достапно на: https://portal.mdt.gov.mk/post-body-files/strateski-dokumenti-mod-file-1eKa.pdf
7. Стратегиски одбранбен преглед 2018 на Република Македонија: Кон членството во НАТО и „Идни вооружени сили 2028“. Достапно на: https://portal.mdt.gov.mk/post-body-files/strateski-dokumenti-mod-file-i3ur.pdf
8. Национална стратегија за безбедност на Република Северна Македонија [National Security Strategy of the Republic of North Macedonia]. Достапно на: https://portal.mdt.gov.mk/post-body-files/nacionalni-strategii-file-O8IL.pdf
9. Институт за комуникациски студии (ИКС) (2025) Справување со СММИ во контекст на регулативите на ЕУ [Документ за јавни политики]. ResPublica. Достапно на: https://respublica.edu.mk/wp-content/uploads/2025/06/policy-paper-addressing-fimi-in-context-of-eu-regulations-en.pdf
10. Институт за комуникациски студии (ИКС) (2025) Странско мешање и манипулација со информации во Северна Македонија. ResPublica. Достапно на: https://respublica.edu.mk/wp-content/uploads/2025/05/foreign-information-manipulation-and-interference-in-north-macedonia.pdf
11. Институт за комуникациски студии (ИКС) (2025) Институционален одговор на странско мешање и манипулација со информации во Северна Македонија: Модели и опции за политика [Документ за јавни политики]. ResPublica. Достапно на: https://respublica.edu.mk/wp-content/uploads/2025/12/institutional-response-to-fimi_en.pdf
12. UK Government Communication Service, RESIST [PDF]. Достапно на: https://www.communications.gov.uk/wp-content/uploads/2025/10/RESIST-FINAL.pdf

Институт за
комуникациски
студии

