ИНСТИТУЦИОНАЛЕН ОДГОВОР НА СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ ВО СЕВЕРНА МАКЕДОНИЈА: МОДЕЛИ И ОПЦИИ ЗА ПОЛИТИКА

ДОКУМЕНТ ЗА ЈАВНА ПОЛИТИКА

Издавач:

Институт за комуникациски студии

ул. „Јуриј Гагарин“ 17-1-1, Скопје

www.iks.edu.mk

За издавачот:

проф. д-р Жанета Трајкоска

Едиција:

ResPublica

Автори:

д-р Александар Грижев, вон. проф.

д-р Весна Попоска, вон. проф.

Уредник:

м-р Дејан Андонов

Лектор:

Ружица Пејовиќ

Графички дизајн:

Ивана Темелкоска

Место и година:

Скопје, 2025

СОДРЖИНА

ИЗВРШНО РЕЗИМЕ 5

ВОВЕД 7

Методологија 9

1. Методолошка рамка и пристап 9

2. Извори на податоци 9

3. Примерок и учесници 10

4. Етика 11

5. Ограничувања 11

ГЛАВА 1: КОН ИНТЕГРИРАН ОДГОВОР НА ИНФОРМАЦИСКИТЕ ЗАКАНИ 12

1.1. Информациските закани и потребата од координиран институционален одговор 13

1.2. Вмешувањето во избори меѓу најсложените операции на СММИ 16

1.3. Респонзивен и аналитички пристап на ЕУ кон СММИ 19

ГЛАВА 2: СОСТОЈБАТА И ПРЕДИЗВИЦИТЕ НА ИНСТИТУЦИОНАЛНИОТ ОДГОВОР НА СММИ ВО СЕВЕРНА МАКЕДОНИЈА 25

2.1. Синтетизирани наоди од квалитативното истражување 26

2.1.1. Општи согледувања и перцепции 26

2.1.2. Институционална поставеност и координација 27

2.1.3. Законска и стратегиска рамка 28

2.1.4. Капацитети и ресурси 29

2.1.5. Перцепција на можностите и предлози за подобрување 29

2.1.6. Клучни предизвици 30

2.2. Анализа на состојбата на системот (GAP Analysis) 31

2.2.1. Институционална поставеност и координација 31

2.2.2. Стратегиска рамка (операционализација) 32
2.2.3. Капацитети и ресурси 33
2.2.4. Стандарди за размена на информации 33
2.2.5. Комуникациска отпорност и писменост 34
2.2.6. Мониторинг и евалуација 34

ГЛАВА 3: КОМПАРАТИВНИ ИСКУСТВА И МОДЕЛИ ЗА ОДГОВОР НА СММИ 35

3.1. Естонија: дигитална држава со рутини за свесност и координација .. 39
3.2. Франција (Viginum): јадрен владин капацитет против дигитални вмешувања 39
3.3. Полска: интерсекторска процена на ризиците и квартални брифинзи 40
3.4. Шведска: Агенција за психолошка одбрана 41
3.5. Финска: писменост, партнерства и превентивни комуникации 41

ГЛАВА 4: ОПЦИИ ЗА ПОЛИТИКА ЗА ОДГОВОР НА СММИ ВО СЕВЕРНА МАКЕДОНИЈА 43

4.1. Опција А: Самостоен центар за национална отпорност 44
4.2. Опција Б: Национален координативен механизам под Владата 45
4.3. Опција В: Зајакнување на постојниот Совет за координација на безбедносно-разузнавачката заедница 47

ГЛАВА 5: ЗАКЛУЧНИ СОГЛЕДУВАЊА И ПРЕПОРАКИ ЗА ИМПЛЕМЕНТАЦИЈА 51

5.1. Заклучни согледувања 52
5.2. Препораки за имплементација 53

ЗА АВТОРИТЕ 56

КОРИСТЕНА ЛИТЕРАТУРА 57

ИЗВРШНО РЕЗИМЕ

Во Северна Македонија постои свесност за ризиците што ги носи странското мешање и манипулирање со информации (СММИ), но системот за координиран одговор во државата останува фрагментиран, без функционална меѓуинституционална координација и јасно дефинирани надлежности. Недостасуваат централизиран механизам за размена на информации, навремена анализа и заедничко реагирање. Повеќето активности се спроведуваат реактивно, во зависност од иницијативата на поединечни институции или сектори, што може да води до преклопување на надлежностите, губење ресурси и неусогласена комуникација со јавноста.

Ограничените капацитети и ресурси, како што се кадар, алатки и буџети за следење, анализа и стратегиска комуникација, и недостигот од систематска едукација во јавниот сектор во доменот на дигиталната и медиумската писменост, ја отежнуваат борбата против СММИ. На ова се надоврзуваат ниското ниво јавна доверба (ИРИ, 2024) и општествена отпорност, поттикнати од поларизацијата и недоволната транспарентност на институционалната комуникација.

Странското мешање и манипулирање со информации не е јасно дефинирано во регулаторната рамка, а постоечките стратегии се недоволно операционализирани преку јасни улоги, протоколи и индикатори за следење и мерење на нивната успешност. Советот за координација на безбедносно-разузнавачката заедница не ги извршува предвидените функции, а во практиката не постои воспоставена структура за брза анализа и заедничка реакција при случаи на дезинформации или странско влијание.

Оттука, клучната препорака на овој документ за јавна политика е дека Северна Македонија треба да воспостави национален механизам за координација и отпорност на СММИ, што ќе обезбеди институционална поврзаност, регулирана размена на информации и системско следење на заканите со јасни улоги, протоколи и индикатори за изведба.

Документот ги нуди следните опции за институционално решение:

- Создавање самостоен центар за дигитална или национална отпорност - подразбира воспоставување независна јавна институција со јасен мандат, одговорности и буџет, која би ги интегрирала функциите на анализа, координација и едукација. Предноста е во централизираната и видлива структура, но моделот бара нови ресурси и административна поставеност.

- **Формирање национален координативен механизам под Владата** - предвидува интегрирање на механизмот преку координативна канцеларија „јадро + мрежа". Така ќе се обезбедат политичка тежина, интероперабилност и брз одговор при кризни ситуации, но потенцијален ризик се преоптовареноста со други прашања,

зависноста од политички континуитет и можниот недостиг од длабока аналитика ако јадрото е мало.

- **Интеграција во Советот за координација на безбедносно-разузнавачката заедница** - овозможува зајакнување и операционализација на постојната структура преку проширување на нејзиниот мандат во областа на СММИ. Предноста е во рационализацијата на веќе воспоставената структура, но ризикот е во пониската јавна видливост и координацијата да остане „на хартија", за што се потребни дисциплина и јасни стандардно-оперативни процедури.

Без оглед на опцијата што би се избрала, овој документ ги предлага следните **препораки за воспоставување стабилен и функционален систем за справување со СММИ**:

- дефинирање институционален модел и носител и именување фокални точки во сите релевантни институции;
- воспоставување редовен календар на активности, разработка на стандардна постапка „пријава – процена - одговор" за управување со инциденти и развивање универзални сценарија и листи за проверка;
- јакнење на човечките капацитети;
- превентивна комуникација за очекуваните манипулативни наративи;
- размена на информации преку заедничка база; и
- воспоставување индикатори за следење на ефикасноста.

Исто така, потребно е институциите да преземат дополнителни мерки и политики што ќе го зајакнат системот и неговата отпорност, како што се:

- ревизија и надградба на постојната Стратегија за отпорност на хибридни закани (2021 – 2025);
- јакнење на институционалните капацитети за следење и анализа;
- воведување програми за медиумска и дигитална писменост во јавниот сектор;
- вклучување на академскиот и граѓанскиот сектор преку формализирани партнерства; и
- поголема интеграција со механизмите на НАТО и ЕУ за борба против СММИ.

Воспоставувањето национален модел за справување со СММИ ќе овозможи на Северна Македонија да премине кон интегриран, функционален и одржлив систем за институционален одговор.

ВОВЕД

Во современиот безбедносен и информативен контекст, странското манипулирање и мешање со информации (СММИ) претставува сериозна и растечка закана за демократските системи, јавната доверба и стабилноста на институциите. Брзиот развој на дигиталните технологии, растечката поврзаност и транснационалната природа на информациските текови овозможуваат ваквите операции да се спроведуваат поефикасно и потешко да се откриваат. Преку употреба на координирани мрежи, прикриени идентитети и генеративна вештачка интелигенција, врз јавното мислење, изборните процеси и надворешната политика на други држави можат да влијаат државни и недржавни актери. Во европски контекст, СММИ се препознава како безбедносна и надворешнополитичка закана што бара координиран, интерсекторски одговор, со акцент не само на содржината, туку и на тактиките, техниките и процедурите на влијание и мешање. Европските институции веќе активираа координирани механизми за зголемена готовност во изборните периоди, што го нагласува значењето на проактивните, а не само на реактивните мерки.

Во Северна Македонија СММИ добива зголемено значење во контекст на евроатлантските интеграции и потребата од јакнење на националната отпорност кон хибридни закани. Во државата постои консензус за значењето на феноменот во рамките на националните политики за хибридни закани и изборен интегритет, засилено со усвојувањето на Националната стратегија за градење отпорност и справување со хибридни закани (2021–2025) и придружниот Акциски план. Како што пишува во стратегијата, отпорноста се засновува на стратегиска ориентација кон интегриран, подобро координиран пристап и градење капацитети на национално ниво, усогласено со НАТО-обврските за цивилна подготвеност и потребите за национална отпорност. Сепак, операционализацијата на стратегијата и акцискиот план остануваат предизвик за институциите, не постои инкриминација на ваквите појави, а институционалниот одговор се соочува со недоволна координација, ограничени човечки и технички ресурси, нејасна распределба на надлежностите и недостиг од систематско следење, анализа и реакција на ризиците.

Во македонскиот правен систем нема експлицитно усвоена дефиниција за странско манипулирање и мешање со информации, што придонесува проблемот да остане делумно неразбран и неадекватно третиран во јавните политики. Од перспектива на политиките и регулативите на ЕУ, терминот опфаќа и содржини и однесувања - во многу случаи СММИ е облик на дезинформација со странско потекло, но вклучува и оперативни тактики и постапки, како што се координирано неавтентично однесување, технички пробиви, протекување материјали и хибридни операции, насочени кон слободното формирање и изразување на политичката волја (Блеер-Симон К., 2025).

Ова двојно сидро - националната рамка за хибридни закани и европската рамка за интегритет на информациската средина, го води и овој документ, односно дефиницијата што се користи е оперативна (заснована на однесувања и процеси) и е насочена кон превенција, детекција и координиран одговор.

Овој документ за јавни политики има цел да го лоцира и да го анализира проблемот на меѓуинституционалната координација за справување со СММИ, како и да предложи конкретни и изводливи решенија за воспоставување на националниот систем за одговор, како дел од пошироките напори за градење институционална и општествена отпорност на хибридните закани. Фокусот е ставен на организациски модели, координациски механизми и инструменти за следење и одговор. Овој комбиниран пристап овозможува да се поврзат наративите и процесите, односно како се одвива влијанието, со институционалните капацитети, односно како да се управува со ризикот со применливи препораки.

Документот се надоврзува на постојната европска и национална рамка, вклучително и обврските што произлегуваат од членството во НАТО и процесот на приближување кон ЕУ. НАТО ја засилува улогата на стратегиската комуникација преку Центарот за извонредност во Рига (*StratCom - NATO Strategic Communications Centre of Excellence*), како поддршка за сојузничките и партнерските земји во градењето капацитети за анализа, комуникација и одвраќање, додека Системот за брзо известување на ЕУ (*Rapid Alert System – RAS*) служи за координација и размена на информации меѓу државите-членки при информативни инциденти. Паралелно, ЕУ воспоставува обврски за управување со системските ризици, вклучително и дезинформациите, за големите онлајн-платформи преку Актот за дигитални услуги (*DSA*) и поставува стандарди за независност и плурализам на медиумите преку Европскиот закон за медиумска слобода (*EMFA*). Конечно, документот се надоврзува на претходните две студии на Институтот за комуникациски студии: Странско мешање и манипулирање со информации во Република Северна Македонија: појдовна анализа (Хаџи-Јанев М., Стоилковски М., 2025) и Осврнување на странското мешање и манипулирање со информации во контекст на европските регулативи (Блеер-Симон К., 2025).

Документот ја опишува тековната состојба („каде сме“) во институционалната поставеност, капацитети и регулаторна рамка, ги идентификува суштинските јазови помеѓу стратегиските намери и фактичката практика, нуди опции за политика (алтернативни институционални модели) засновани на компаративни искуства и предлага патоказ за имплементација. Оттука, тој е структуриран во следните целини:

Глава 1: Кон интегриран одговор на информациските закани;

Глава 2: Состојбата и предизвиците на институционалниот одговор на СММИ во Северна Македонија;

Глава 3: Компаративни искуства и модели за одговор на СММИ;

Глава 4: Опции за политика за одговор на СММИ во Северна Македонија; и

Глава 5: Заклучни согледувања и препораки за имплементација.

Со оваа структура документот им овозможува на носителите на одлуки, експертите и пошироката јавност да ги согледаат тековните институционални ограничувања и да препознаат конкретни насоки за развој на интегриран, проактивен и координиран систем на отпорност кон странското мешање и манипулирање со информации.

Методологија

1. Методолошка рамка и пристап

Анализата се засновува на комбиниран методолошки пристап што поврзува (1) деск-анализа на релевантни национални и на ЕУ и НАТО политики и документи (2) квалитативни наоди од фокус-групи и интервјуа со претставници од клучни институции; (3) анализа на состојбата (*GAP analysis*) на институционалниот систем; и (4) компаративна анализа на добри практики од држави-членки на ЕУ и НАТО (Естонија, Финска, Франција, Полска и Шведска). Целта е да се добие интегрирана слика: (а) како СММИ се манифестира и се перципира во практиката; (б) колку институционалната рамка и капацитетите овозможуваат ефикасен одговор; и (в) кои модели се применливи во Северна Македонија. Резултатите од анализата служат како основа за развој на препораки за политика, кои ќе овозможат градење посеопфатен и интегриран систем за спречување и управување со ризиците од СММИ.

2. Извори на податоци

(а) Деск-анализа. Прегледани се релевантни регулативи и политики на ЕУ и НАТО (Актот за дигитални услуги - *DSA*; Европскиот закон за медиумска слобода - *EMFA*; Стратегискиот концепт на НАТО (2022); Сет на алатки за одговор на СММИ (*FIMI Toolbox*), Систем за брзо предупредување (*Rapid Alert System - RAS*) и др.), Националната стратегија за градење отпорност и справување со хибридни закани (2021–2025) со акцискиот план, како и претходни публикации на ИКС, за да се обезбеди нормативно-политичкиот контекст. Резултатите од деск-анализата се триангулирани со наодите од фокус-групите за да се изгради кохерентна интерпретација на системските јазови, а со комбинирањето на изворите и техниките да се зголеми и валидноста на наодите (Bryman, 2016). Во дизајнот на следење и евалуација се водевме од насоките на Организација за економска соработка и развој (*OECD*) за мониторинг и евалуација на јавни политики (OECD, 2017).

(б) Фокус-групи. Во септември 2025 година спроведени се две фокус-групи со претставници од клучни институции и регулатори. Дискусиите беа полуструктурирани според водич со пет тематски целини: разбирање на СММИ, институционална координација, законска или стратегиска рамка, капацитети и ресурси и меѓународна соработка. Сесиите се одржаа во контролирана средина (90-120 минути), со модерирање од истражувачки тим, а записите беа водени како белешки и транскрипти. Испитаниците што не можеа да учествуваат во фокус-групите одговорија на прашалник за интервјуа. Исказите во документот се парафразирани за да се илустрираат повторувачки тенденции, а наодите се прикажани како преглед на заедничките согледувања и системски предизвици, со цел да се извлечат аналитички поенти за тековното ниво на институционална зрелост и отпорност.

(в) Анализа на состојбата (*GAP analysis*). Извршена е споредба меѓу стратегиските намери и обврски и реалната институционална практика во однос на улогите и надлежностите, процесите на координација и размена на информации, кадровските и техничките ресурси и механизмите за следење и евалуација. Јазовите се сумирани по домени и се користат како мост кон политичките опции и патоказот за имплементација.

(г) Компаративна анализа. Селектирани се пет референтни модели од држави-членки на ЕУ и НАТО (Естонија, Финска, Франција, Полска и Шведска) според следните критериуми за применливост: јасно дефиниран мандат и процеси, интерсекторска координација, алатки и кадар, транспарентна стратегиска комуникација и мерливи резултати.

3. Примерок и учесници

Квалитативното истражување користеше „намерен примерок" (*purposive sampling*), каде што релевантноста на учесникот за истражувачката цел има предност пред статистичката репрезентативност (Bryman, 2016). Примерокот опфати различни нивоа на јавната администрација (стратегиско, оперативно и аналитичко), со цел да се обезбеди повеќеслоен увид во процесите на планирање, спроведување и евалуација. Застапеноста на претставници од владини координациски структури, безбедносно-разузнавачки сектори, дипломатско-конзуларниот ресор и од ресорите за дигитална трансформација, јавна администрација, ИКТ-безбедност и за медиумска регулација, овозможи да се споредат институционалните перспективи (нормативна и организациска) со оперативните искуства (реални процедури, тесни грла, ограничувања). Во истражувањето беа вклучени следните институции: министерствата за надворешни работи, за внатрешни работи, за дигитална трансформација и за јавна администрација, Националниот комитет за спречување насилен екстремизам и борба против тероризмот, Агенцијата за разузнавање (АР),

Агенцијата за аудио и аудиовизуелни медиумски услуги (АВМУ), Националниот центар за сајбер инциденти (МКД-ЦИРТ), Центарот за управување со кризи и Управата за наменско производство при Министерството за економија.

4. Етика

Со оглед на чувствителноста на темата, особено за институции со безбедносни надлежности, истражувањето се спроведе според јасни етички протоколи. Сите учесници беа информирани за целта, начинот на користење на податоците и мерките за заштита на идентитетот. Во извештајот не се наведуваат имиња, должности или конкретни институции за да се зачува доверливоста и да се избегне имплицитна атрибуција на ставови на конкретна институција. Сегментите што би можеле да упатат на специфични оперативни практики се агрегираат на тематско ниво, а заклучоците се формулираат како синтеза на повторувачки тенденции, а не како поединечни тврдења. Со ова се намалуваат ризиците од погрешна интерпретација и се зачувува доверливоста без да се компромитира аналитичката вредност.

5. Ограничувања

Вообичаено за квалитативните студии, фокус-групите не претендираат репрезентативност, туку обезбедуваат длабинско разбирање на процесите и перцепциите. Употребата на парафразирани цитати ја намалува можноста за буквално цитирање, но истовремено овозможува да се задржи суштината на аргументацијата. Потенцијалната пристрасност на социјално посакуваното однесување е ублажена преку модераторски техники (разложување на прашања, барање конкретни примери, насочување кон процеси наместо кон лични ставови) и преку триангулација со документи и компаративни искуства. Конечните тврдења во документот се темелат на конвергенција помеѓу повеќе извори, а не на единечни искази (Bryman, 2016).

ГЛАВА 1:

КОН ИНТЕГРИРАН ОДГОВОР НА ИНФОРМАЦИСКИТЕ ЗАКАНИ

1.1. Информациските закани и потребата од координиран институционален одговор

Странското мешање и манипулирање со информации (СММИ) го опфаќа спектарот од содржински и, уште поважно, бихејвиорални практики со кои странските актери се обидуваат да ја нарушат или да ја насочат јавната расправа, да влијаат врз демократските процеси и да ја еродираат довербата во институциите. Во европскиот пристап СММИ не се третира само како „штетна содржина", туку и како тактики, техники и процедури (*TTPs*), како што се хакирање и објавување (*hack-and-leak*), компјутеризирани лажни информации, координирани неавтентични активности итн. (Блеер-Симон К., 2025). Во литературата ова дополнително се опишува како когнитивни операции и алгоритамско влијание врз јавната сфера (Pamment, 2020). Современите активни мерки функционираат како долгорочни кампањи со препознатливи шаблони на однесување (Rid, 2020). Овој поим е поставен во рамката на пошироките хибридни закани (Hoffman, 2007), за кои националната стратегија бара поинтегриран и подобро координиран одговор на национално ниво, со јасни улоги и механизми за отпорност.

Дефиницијата за СММИ според Европската служба за надворешно дејствување (*The European External Action Service - EEAS*) е: „СММИ претставува претежно ненелегален образец на однесување што претставува закана или има потенцијал негативно да влијае врз вредностите, процедурите и политичките процеси. Таквите активности се манипулативни по својата природа, се спроведуваат на намерен и координиран начин. Актери во овие активности може да бидат државни или недржавни субјекти, вклучително и нивни посредници, како во рамките на нивната територија, така и надвор од неа" (EEAS, 2025).

- *„Претежно ненелегален"* - ова го отежнува справувањето со феноменот преку постоечката правна рамка и се создава притисок врз законодавците да воспостават нови сетови на правила.

- *„Образец на однесување"* - додека активностите за спротивставување на дезинформациите често се фокусираат на содржината и наративите, оваа дефиниција го пренасочува фокусот од содржината кон однесувањето, бидејќи СММИ претставува намерна манипулација со информациите. Образецот на тактики, техники и процедури (*TTPs*) води и кон идентификација на актерите на заканите.

- *„Се заканува или потенцијално влијае врз вредностите, процедурите и политичките процеси"* - СММИ е стратегиско по својата природа и ја опфаќа секоја манипулација со информации што може да предизвика јавна штета, а се приоритетизираат четири главни домени:

- Политичка дезинформација, која има тенденција да фаворизира една страна во политичката конкуренција или да ја поткопа довербата во институциите и демократскиот процес.
- Здравствена дезинформација, која ги загрозува заедниците.
- Еколошка дезинформација, особено поврзана со климатските промени.
- Дезинформација што може да претставува безбедносна закана или да го наруши јавниот ред.

- *„Манипулативни, намерни и координирани"* - операциите за СММИ користат манипулативни тактики со цел да измамат, да доведат во заблуда и да ја дестабилизираат својата цел. Целите најчесто се демократски општества, но странското мешање и влијание се присутни на глобално ниво, вклучително и во земјите во развој.

Актерите на СММИ имаат цел да предизвикаат поларизација во општеството преку промоција на екстремни ставови заради продлабочување на конфликтите, што пак го отежнува демократскиот дијалог. Тие манипулираат со содржината со изменување на автентични информации или медиуми, како што се уредување слики или видеа заради промена на нивното значење, и создаваат фабрикувана содржина, како лажни веб-страници што имитираат легитимни извори, длабински лажни видеа (*deep fake*) и аудио и визуелни материјали генерирани со вештачка интелигенција. Освен тоа, креираат лажни наративи, имитирајќи личности и злоупотребувајќи дипломатски или институционални профили на социјалните мрежи, паралелно дискредитираат доверливи извори и го преформулираат контекстот за да се збунат публиките, а амплификацијата ја вршат преку употреба на ботови, тролови или координирани мрежи за вештачко зголемување на видливоста и кредибилитетот на дезинформацијата. Истовремено, се користат сајбер алатки, вклучително и хакирање и други активности за кражба, измена или фабрикување на информациите (Поповска В., 2024).

СММИ се појавува преку спој од наративи (како се врамува темата и кои емоции се активираат), канали (традиционални медиуми, онлајн платформи, апликации за пораки) и техники (планирани тактики и постапки). Типични примери се:

- координирано неавтентично однесување на социјалните мрежи (усогласени објави, лажни профили/„ботови", вештачко создавање тренд);
- „хакирање и објавување" материјали непосредно пред чувствителни настани (избори, кризи), за насочување на вниманието и нарушување на довербата;
- посреднички организации и медиуми со нетранспарентно финансирање, вклучително и практики на медиумско заробување (контрола врз уредувачките политики и сопственоста);

- манипулирање со видливоста на содржините на платформите (наместено рангирање, „инсценирана“ граѓанска поддршка, вештачко зголемување на досегот);
- комбинирање со други хибридни инструменти (сајбер напади, економски притисок, дипломатско врамување) за поголем ефект.

Овие практики тешко се решаваат само со мерки насочени кон поединечни содржини. Затоа **акцентот се става на проценка на ризикот и јасни постапки за одговор кај државните органи и платформите, во рамките на пошироката политика за хибридни закани и институционална отпорност** (Блеер-Симон К., 2025).

Оттука, генерално, **државите самостојно, во согласност со проценките за ризиците, националните безбедносни стратегии и одбранбените доктрини треба да ги дефинираат, детектираат и да им се спротивстават на ваквиот тип закани**.

Во рамките на НАТО, пристапот се фокусира на „информациски закани“ – намерни, штетни, манипулативни и координирани активности што ги спроведуваат државни и недржавни актери, вклучувајќи непријателски информациски операции, манипулација со информации, вмешување од страна на странски актери и дезинформации распространети преку традиционални и социјални медиуми (NATO, 2020). Алијансата тесно соработува со сојузниците и партнерите за да ги разбере, спречи и да изгради отпорност кон овие информациски закани. Одговорите на НАТО опфаќаат проактивни краткорочни, среднорочни и долгорочни мерки, базирајќи се на четири клучни функции: (1) разбирање на информациската средина (*Understand*), (2) спречување на ефективноста на информациските закани (*Prevent*), (3) ограничување и ублажување на специфични информациски инциденти (*Contain and Mitigate*) и (4) закрепнување и извлекување поуки (*Recover*). **Проактивната комуникација е една од клучните алатки за спротивставување на информациските закани.** НАТО алијансата комуницира со целните публики преку различни канали (официјална веб-страница, редакција и соопштенија за јавноста, Преглед на НАТО, поткасти, официјални профили на Икс, Фејсбук, Инстаграм, Јутјуб и Линкдин), обезбедувајќи точни информации што им помагаат на луѓето да ги препознаат и да им се спротивстават на информациските закани. Овој проактивен пристап кон објаснување и превентивно расчистување на наративите (*prebunking*) е усогласен со рамката за инфоекологија и класификацијата на видови дезинформации (Wardle & Derakhshan, 2017). Истражувањата покажуваат дека кратките предупредувања пред изложувањето ја зголемуваат отпорноста кон манипулативни наративи (Banas & Miller, 2013).

Европските регулативи, како што се Актот за дигитални услуги (DSA) и Европскиот закон за медиумска слобода (EMFA) додаваат системско гледиште (European Commission, 2020): наместо еднократни реакции на поединечни содржини, тежиштето

е на управувањето со системските ризици, заштитата на медиумскиот плурализам и интероперабилните механизми за известување и координација (Блеер-Симон К., 2025). Тоа подразбира дека **ефективниот одговор на СММИ мора да комбинира институционална координација, оперативни протоколи и комуникациска отпорност, а не само законски забрани или технички мерки**.

1.2. Вмешувањето во избори меѓу најсложените операции на СММИ

Едно истражување за граѓанството и демократијата на Евробарометар од декември 2023 година покажа дека 81 процент од граѓаните на ЕУ веруваат дека странското мешање во демократските системи претставува сериозен проблем што треба да се реши, а 78 проценти се загрижени дека дезинформациите можат да влијаат врз одлуките за гласање на луѓето (European Commission, 2023). Порано ограничено на заплашување, изборна измама или хакерски напади, денес мешањето опфаќа и многу поневини, но сеприсутни и секојдневни интеракции. Еден наизглед безопасен и случаен разговор сега може да се смета за дел од кампања за непријателско влијание.

Германската влада на 30 декември 2024 година обвини дека Илон Маск се обидува да влијае врз изборите преку отворена поддршка за политичката партија Алтернатива за Германија (*AfD*), по што администрацијата на Бундестагот во јануари и февруари 2025 година покрена проверка дали таквата поддршка би можела да се смета за незаконска партиска донација. Маск претходно објави колумна во германскиот весник „*Welt am Sonntag*" со пофалби за *АфД* и на 9 јануари 2025 година учествуваше во разговор во живо на Икс со колидерката на партијата Алисе Вајдел (на платформата има над 200 милиони следбеници). Паралелно, Европската комисија во рамките на постојната постапка за прекршување на Европскиот закон за дигитални услуги (*DSA*) против Икс (на 9 и 17 јануари 2025 година) спроведе дополнителни проверки и побара документација за алгоритмите и одржаниот разговор во живо (Reuters, 2025).

По избувнувањето на војната во Украина во 2022 година, Русија започна обемна кампања на дезинформации насочена кон дестабилизација на ЕУ и нејзините членки. Како одговор, ЕУ воведе санкции против руските средства и актери вклучени во СММИ. На 8 октомври 2024 година беа донесени дополнителни рестриктивни мерки против дестабилизирачките активности на Русија, меѓу кои и поткопување изборни процеси, нарушување на функционирањето на демократските институции и координирани напади со дезинформации и странско мешање.

За време на изборите во Бразил во 2022 година дезинформациите ширени преку Вотсап (*WhatsApp*) и Телеграм (*Telegram*) значително влијаеја врз ставовите на гласачите. Судот за изборен надзор (*TSE*) често бараше отстранување содржини, а беше активиран и чет-бот за проверка на факти. Истражувањата покажаа дека овие платформи овозможиле масовно ширење лажни информации, особено за електронските гласачки машини, што доведе до недоверба во изборниот процес и зголемени тензии (Mozilla Foundation, 2024).

Примери за вмешување во изборните и други клучни државни процеси се забележуваат и во регионот.

На претседателските избори во Романија одржани на 24 ноември 2024 година ултранационалистичкиот проруски кандидат Калин Ѓоргеску водеше во првиот круг со 22,94 проценти од гласовите. Овој исход ги поби предизборните анкети, кои предвидуваа неговата поддршка да биде помеѓу 5 и 10 проценти. Ѓоргеску, гласен критичар на НАТО и ЕУ, го надмина актуелниот премиер Марсел Чолаку, кој обезбеди само 19,5 проценти од гласовите, што е прв случај во посткомунистичка Романија социјалдемократ (PSD) да не успее да стигне до вториот круг. Кампањата на Ѓоргеску беше обележана со сомнителен пораст на активноста на социјалните медиуми, особено на Тикток и Телеграм, поттикната од платени инфлуенсери и координирана мрежа на профили на социјалните платформи. Романските разузнавачки служби откриј дека актери поврзани со Русија одиграле клучна улога во засилувањето на проруските и антизападните наративи. Тикток отстрани милиони лажни профили што ги промовираа пораките на Ѓоргеску, иако кампањата веќе нанесе значителна штета. Проценките на разузнавањето потврдија дека многу од овие профили биле поврзани со субјекти поврзани со Русија, што докажува директна вмешаност на Москва во манипулирањето на јавното мислење. На 6 декември 2024 година Уставниот суд на Романија презеде невиден чекор со поништување на резултатите од изборите поради широко распространети нерегуларности и веродостојни сомневања за странско мешање (House of Commons Library, 2024).

За време на прес-конференција во март 2025 година косовскиот премиер Албин Курти изјави дека српскиот претседател Александар Вучиќ интервенирал во парламентарните избори во Косово преку српската влада, разузнавачките служби и групи на организираниот криминал. Курти, исто така, спомена дека Милан Радојичиќ, поранешен заменик-лидер на партијата Српска листа, одиграл значајна улога во мешањето. Радојичиќ ја презеде одговорноста за организирањето на нападот во селото Бањска во општината Звечан, со мнозинско српско население, на северот од Косово, на 24 септември 2023 година. Косово побара негова екстрадиција од Србија. Во реакција на Фејсбук Српска листа ги отфрли обвинувањата од Курти и Рашиќ, нарекувајќи ги „брутални лаги". „Српска листа е горда што доби најголема поддршка од српскиот народ и што, и покрај сите притисоци, уцени и закани, успеа да се спротивстави благодарение на единството на нашиот народ, уште еднаш докажувајќи дека нема да има предавање", објави партијата. Мисијата за

набљудување на изборите на Европската Унија на 11 февруари 2025 година, за време на презентацијата на прелиминарните наоди за одржаните избори, изјави дека Србија се мешала во изборите преку притисок врз српските гласачи во Косово (EU EOM, 2025).

Локалните избори во Никшиќ во 2021 година претставуваа пресвртна точка за Црна Гора, особено поради силното вклучување на соседна Србија во изборната кампања. Присуството на членови на владејачката партија во Србија, Српската напредна партија (СНС), или на личности блиски до нив, предизвика загриженост. Некои од нив беа приведени, а други добија забрана за влез во земјата поради сомневање дека внеле пари за купување гласови. По завршувањето на изборите, Градот Белград, како што беше ветено во кампањата, дониираше два милиони евра на општината Никшиќ, што дополнително ги засили сомневањата за прекршување на изборниот интегритет и странско влијание (CDT, 2024).

Црна Гора се соочи со политички превирања и непосредно пред пристапувањето во НАТО, но и потоа, кои беа последица на различни навидум општествени прашања, а најизразени беа оние што се поврзуваа со верските прашања. Фазата на деморализација вклучуваше огромно присуство на лажни информации, говор на омраза, дезинформации и повици за одбрана од замислен непријател. Во дезинформациската кампања, еден веб-портал одигра водечка улога создавајќи сериозен квантум на дезинформации. Веб-порталот, иако не беше регистриран во регистарот на медиуми, се претставуваше како информативен медиум. Притоа, креираше многу содржини насочени да предизвикаат емоционална реакција од публиката, користејќи злоупотреба на историските контексти и поврзувајќи го претседателот на Црна Гора со фашистичките режими од Втората светска војна. Слично постапуваше и рускиот провладин медиум Спутник. Случаите на дезинформации од страна на овие два портали беа документирани од дигиталниот форензички центар во Подгорица (IREX, 2023).

Од оваа перспектива, **мешањето не се однесува толку на начинот на кој се гласа, туку на обликувањето на мотивациите, намерите и контекстите во кои гласачите размислуваат за политиката.** А токму тие процеси – дебатите, убедувањата и хаотичните расправии, се суштински дел од демократијата.

1.3. Респонзивен и аналитички пристап на ЕУ кон СММИ

Европската Унија располага со развиена и сеопфатна инфраструктура што овозможува операционализација на активности насочени кон градење отпорност кон странското малициозно влијание. Оваа инфраструктура се темели на повеќе стратегиски документи, регулативи и механизми. Преку овие инструменти ЕУ не само што ги дефинира стандардите за идентификација и спротивставување на странското мешање и манипулирање со информации и хибридни закани, туку и воспоставува конкретни оперативни механизми за координација меѓу институциите, мониторинг на ризиците и ангажирање на приватниот сектор и граѓанското општество. Освен тоа, преку Европската служба за надворешно дејствување (EEAS) и специјализираните тимови како Хибридна фузиска единица на ЕУ (EU Hybrid Fusion Cell) и Стратком работни групи (StratCom Task Forces), се овозможуваат навремено собирање, анализа и дистрибуција на информации за потенцијални влијанија, со цел да се поддржат земјите членки и партнерите во развојот на сопствени капацитети за отпорност. Интероперабилноста во меѓународните мрежи ја засилува отпорноста во меѓузависната средина (Keohane & Nye, 1998).

Меѓу механизмите што му се на располагање на Советот на ЕУ се издвојуваат:

- **сет алатки за одговор на СММИ (FIMI Toolbox, EEAS);**
- **сет хибридни алатки, вклучително и тимови за брз одговор на хибридни закани (Hybrid Toolbox; Hybrid Rapid Response Teams - HRRTs);**
- **сет алатки на ЕУ за сајбер дипломатија (EU Cyber Diplomacy Toolbox);**
- **Европската мрежа за соработка на избори (European Cooperation Network on Elections - ECNE);**
- **Кодексот за практики против дезинформации (Strengthened Code of Practice on Disinformation, 2022);**
- **Системот за брзо предупредување (Rapid Alert System RAS);**
- **Европската опсерваторија за дигитални медиуми (European Digital Media Observatory - EDMO).**

Освен тоа, ЕУ има усвоено неколку **акти и директиви** заради зголемување на одговорноста на онлајн платформите, зајакнување на сајбер безбедноста, отпорноста на дигиталната инфраструктура и за регулирање на употребата на нови технологии во комуникацијата. Овие легислативи ги вклучуваат:

- **Актот за дигитални услуги (Digital Services Act - Regulation (EU) 2022/2065);**

- **Актот за вештачка интелигенција (Artificial Intelligence Act - Regulation (EU) 2024/1689);**
- **Директивата за отпорност на критични субјекти (Directive (EU) 2022/2557);**
- **Директивата за мрежна и информациска безбедност (NIS2 – Directive (EU) 2022/2555);**
- **Регулативата за транспарентност и таргетирање на политичкото рекламирање (Regulation (EU) 2024/900);**
- **Актот за слобода на медиумите во Европа (European Media Freedom Act – Regulation (EU) 2024/1083).**

Овие мерки се наведени во заклучоците на Советот на Европа од мај 2024 година за заштита на изборните процеси од странско мешање и во заклучоците на Претседателството од мај 2025 година за зајакнување на демократската отпорност.

ЕУ разви два клучни механизми за справување со странско информациско влијание: сет алатки за одговор на СММИ (*FIMI Toolbox*) и Систем за брзо предупредување (*Rapid Alert System - RAS*), кои може да се преземаат и да се имплементираат со адаптација на националните потреби и контекст (EU StratCom Task Force, 2022).

Сетот од алатки за одговор на СММИ креиран од Европската служба за надворешно дејствување е концептуален и оперативен рамковен механизам, повеќе превентивен отколку реактивен, и се темели на четири столба:

1. ситуациска свесност - преку мониторинг, анализа и техники на собирање информации од јавни или други отворени извори (*OSINT*) се идентификуваат наративите, изворите и методите на манипулација;
2. отпорност - се гради капацитет кај граѓаните, медиумите и институциите да ги препознаваат и да ги одбиваат дезинформациите;
3. регулатива - се развиваат политики и законски механизми за санкционирање и превенција;
4. надворешна акција - дипломатски одговори, поддршка на партнерите и глобална координација.

Системот за брзо предупредување (*RAS*) е дигитална платформа што функционира како информациски аларм - кога се детектира дезинформациска кампања, системот овозможува брза размена на информации меѓу земјите членки, институциите и партнерите. Механизмот вклучува мрежа од национални фокални точки што се поврзани во реално време и овозможува интеграција на податоци од медиуми, проверувачи на факти, академски извори и од технолошки платформи. Координираните одговори може да бидат јавни комуникации, дипломатски реакции или технички интервенции.

Европската служба за надворешно дејствување воспостави и напредна **аналитичка рамка за заканите од СММИ**, која може да послужи како модел за тоа како треба да се структурира процесот на набљудување, анализа и размена на информациите меѓу институциите (EEAS, 2023; EEAS, 2024). Аналитичката рамка претставува интегриран систем што обединува методолошки (ABCDE), процесни (аналитички циклус), технички (DISARM) и структурни (STIX) елементи:

- **ABCDE.** Рамковниот модел ABCDE претставува основен пристап за диференцирање на инцидентите од СММИ според пет димензии: актер (Actor), однесување (Behaviour), содржина (Content), степен (Degree) и ефект (Effect). Неговата примена во национален контекст би овозможила создавање стандарди за анализа на инциденти од СММИ, препознавање повторливи шеми и развој на контрамерки.

Табела 1: Рамка ABCDE за анализа на СММИ

Елемент	Прашање	Цел
Актер (Actor)	Кои типови актери се вклучени?	Да се утврди дали инцидентот вклучува странски државен или недржавен актер.
Однесување (Behaviour)	Кои активности се забележани?	Да се идентификуваат докази за координација, намера и користени техники.
Содржина (Content)	Каков вид содржина се создава и се дистрибуира?	Да се утврди дали информацијата е измамничка, манипулативна или делумно точна.
Степен (Degree)	Колкава е распространетоста на содржината?	Да се анализираат целните публики и обемот на дистрибуција.
Ефект (Effect)	Какво е влијанието и кого го засегнува?	Да се процени реалната штета и сериозноста на случајот.

- **Аналитички циклус.** Европската служба за надворешно дејствување ја надградува оваа рамка преку воспоставување аналитички циклус, кој овозможува стратегиски и самоодржлив процес на набљудување, анализа и надградување на институционалното знаење. Фазите на аналитичкиот циклус опфаќаат:

1. Стратегиско следење (Strategic Monitoring) - се мапира екосистемот на познати ресурси што ги користат актерите на заканите, се следат шемите на засилување и новите канали на дистрибуција.
2. Приоритетизација и тријажа (Prioritisation and Triage) - се селектираат инцидентите од највисок приоритет, особено оние што имаат директно политичко или безбедносно значење.
3. Анализа и собирање докази (Incident Analysis and Evidence Collection) - се прави анализа на поврзаноста на каналите и содржините, а доказите се архивираат во согласност со Општата регулатива за заштита на податоците (General Data Protection Regulation - GDPR) и Беркли протоколот за дигитални истраги базирани на отворени извори (Berkeley Protocol on Digital Open-Source Investigations).
4. Споделување знаење (Knowledge Pooling and Sharing) - резултатите се споделуваат со релевантни институции и партнери заради брза реакција и градење колективна свесност.
5. Ситуациска свесност (Situational Awareness) - се ажурира база на податоци, се додаваат нови актери и техники, а преку компаративна анализа се извлекуваат долгорочни трендови.

- DISARM. За да се операционализира елементот „B" од рамката ABCDE, односно однесувањето на актерите зад СММИ, Европската служба за надворешно дејствување ја користи рамката DISARM. Таа е заеднички, отворен и адаптибилен систем за категоризација на техниките, тактиките и процедурите (TTPs) што ги користат актерите на заканите, овозможувајќи идентификација на нивните повторливи техники и тактики и рано откривање и прекинување на нивните операции. Рамката DISARM ги дели фазите на еден инцидент на СММИ на:

1. Планирање (Planning) - дефинирање на целта и очекуваното влијание.
2. Подготовка (Preparation) - создавање инфраструктура и избор на канали.
3. Извршување (Execution) - спроведување на операцијата преку координирани активности.
4. Оценување (Assessing) - мерење на ефектот и приспособување на стратегијата.

- STIX™. И конечно, за да се обезбеди споделувањето на информациите за заканите, Европската служба за надворешно дејствување ги кодира инцидентите на СММИ во форматот STIX™ (Structured Threat Information Expression). Примената на овој формат овозможува интероперабилност меѓу институциите и интегрирање делумни информации во поголема аналитичка слика. На тој начин, секој идентификуван наратив или техника придонесува за создавање ситуациска свесност и рано предупредување. Овој формат, првично развиен за сајбер безбедност, овозможува претставување на сите релевантни објекти и врски во еден инцидент на СММИ.

Табела 2: Формат STIX™ (Structured Threat Information Expression)

STIX објект	Опис
Инцидент (Incident)	*Ги содржи основните информации за инцидентот (име, опис, почетен датум, цел итн.)*
Набљудувано (Observable)	*URL или датотека што била забележана во рамките на инцидентот.*
Канали - ширење (Channels extension)	*Секој онлајн или офлајн комуникациски канал (веб-страница, профил или страница на социјални медиуми, ТВ-станица итн.) што ги објавува набљудуваните елементи.*
Идентитет (Identity)	*Поединци, организации или локации, вклучувајќи држави. Обично ги опфаќа целите на инцидентите.*
Заканувачки актер (Threat Actor)	*Содржи информации за актерите што претставуваат закана.*
Настан - ширење (Event (extension))	*Опис на реален настан, како избори, емисија, годишнина итн., за да се обезбеди контекст во кој може да се случуваат инцидентите.*
Ранливост (Vulnerability)	*Опис на ранливоста што била искористена за да се овозможи изведбата на инцидентот.*
Јазик – ширење (Language (extension))	*Јазикот/јазиците што бил/е користен/и во инцидентот.*
Шема на напад (Attack Pattern)	*Опис на манипулативни техники (TTPs) што се користат за изведување на нападот.*
Мерка за дејствување (Course of Action)	*Опис на контрамерки против инцидентот.*
Наратив – ширење (Narrative (extension))	*Опис на наративите што се користат во инцидентите. Наративите може да бидат вгнездени и претставени како мета- и поднаративи.*

Аналитичката рамка на Европската служба за надворешно дејствување, приспособена на националните специфики и институционалната структура, може да стане темел на националниот систем за рано предупредување и одговор на СММИ, што би им овозможил на институциите да воспостават заедничка методологија и терминологија за анализа на информациските инциденти, да создадат унифицирана база на податоци за актерите, техниките и содржините, да овозможат координирани и навремени реакции и долгорочно да развиваат капацитети за предвидување и превенција.

ГЛАВА 2:

СОСТОЈБАТА И ПРЕДИЗВИЦИТЕ НА ИНСТИТУЦИОНАЛНИОТ ОДГОВОР НА СММИ ВО СЕВЕРНА МАКЕДОНИЈА

2.1. Синтетизирани наоди од квалитативното истражување

2.1.1. Општи согледувања и перцепции

Меѓу државните чинители во Северна Македонија постои свесност за генералната проблематика на хибридните закани, дезинформациите и потенцијалот за странско штетно влијание. Се согледува дека Северна Македонија се наоѓа во високоизложено регионално опкружување, каде што информациските влијанија, особено оние со надворешно потекло, често се надоврзуваат на постојните политички и општествени поделби. Сепак, **нивото на разбирање на проблематиката е различно и, очекувано, повисоко е кај претставниците на безбедносно-разузнавачката заедница**. Странското мешање и манипулирање со информации се препознава како сложен и динамичен феномен што се наоѓа на пресекот меѓу безбедносните, информациските и комуникациските политики. Но со оглед на тоа дека оваа закана не е дефинирана во домашната регулатива, таа сè уште нема унифицирано институционално разбирање. Дел државни чинители го идентификуваат СММИ првенствено преку призмата на сајбер напади, онлајн пропаганда и манипулативни содржини, додека други го поврзуваат со пошироки форми на странско влијание и дестабилизирачки комуникациски практики. Оттука, **извесна е потребата од интервенција во рамката за градењето политики**.

Во државата **постои основна институционална инфраструктура, но неопходно е изолираните точки да се поврзат во систем** што функционира кохерентно и одлучно, со прецизно определени надлежности и активности. Иако СММИ се воочува како реална и растечка закана за демократските процеси и националната безбедност, институциите во најголем дел пристапуваат селективно и во зависност од контекстот, при што активностите најчесто се фокусирани на тековни кризни ситуации (изборни процеси, дезинформациски кампањи или регионални настани), а не во рамките на континуиран, системски механизам за превенција и отпорност. Не сите чинители ја препознаваат својата улога во поширокиот систем, а повеќето посочуваат на отсуство на институционална комуникација и меморија, како и недостиг од човечки и технички капацитети. Најголем дел не ги препознаваат своите институции ниту како носители на одговорност или надлежности во тој дел, што подразбира дека **е потребна интервенција и на стратегиско и на политичко ниво**.

Процесите што се започнати во Министерството за дигитална трансформација во насока на апроксимација на европските директиви за безбедност на мрежите и Актот за дигитални услуги (*DSA*) **се очекува да дадат силни резултати во поглед на зголемената сајбер отпорност**, а веќе воспоставената **соработка со партнерските земји и организации се смета за клучна во надминувањето на предизвиците**.

Најголем дел **државни чинители не беа запознаени со постоењето на акцискиот план поврзан со Стратегијата за градење отпорност од хибридни закани**, а дел посочија дека одговорностите што им се доверени со стратегијата не се дел од нивната институционална надлежност. Иако не е познато дали постои механизам за следење на имплементацијата на акцискиот план поврзан со Стратегијата, воочливо е дека таа ги нема остварено проектираните резултати, заради што **е потребна длабинска анализа при подготовката на следниот стратегиски и/или акциски документ во циклусот**.

Ова укажува дека **државните институции се наоѓаат во различни фази на институционално усвојување на концептот за СММИ**: од основна свесност, преку развивање интерни капацитети, до практична интеграција во стратегиските документи и оперативните политики. Тоа подразбира дека свесноста, знаењето и одговорот за странското мешање и манипулирање со информации се **област во која е потребна надградба**. Институциите препознаваат дека градењето општествена отпорност кон СММИ бара долгорочен пристап што ги надминува административните и техничките рамки и се потпира на партнерство со академскиот и граѓанскиот сектор и медиумите. Затоа, систематската едукација во областа на **медиумската и дигиталната писменост и транспарентната и отчетната комуникација** е клучна за подигнување на степенот на отпорноста кон ваков тип закани.

2.1.2. Институционална поставеност и координација

Во моменталниот институционален контекст постои потреба од воспоставување систематизиран и одржлив механизам за координација меѓу релевантните актери. Иако постојат одредени форми на меѓуинституционална комуникација, тие главно се базираат на неформални релации и лични контакти, што создава ризик од недоследност, ограничена транспарентност и зависност од индивидуалните капацитети. Овој пристап, иако понекогаш ефикасен во краток рок, не обезбедува долгорочна институционална стабилност и предвидливост во процесите на одлучување и имплементација. И покрај тоа што Стратегијата за градење отпорност од хибридни закани и нејзиниот акциски план предвидуваат воспоставување структури и механизми за редовна размена на информации и координација, Советот за координација на безбедносно-разузнавачката заедница, кој формално е предвиден како координативно тело, не одржува редовни состаноци и нема видливи резултати во областа на СММИ.

Во отсуство на активен централизиран механизам, институциите реагираат ад хок, во рамките на своите надлежности, што резултира со фрагментиран систем на одговор. Поединечни институции спроведуваат ограничени активности како кампањи за медиумска писменост, мониторинг на дезинформациски содржини или активности поврзани со заштита на критичната информациска инфраструктура,

но овие напори се одвиваат изолирано, без заедничка рамка за координација и споделување информации.

Ваквата состојба не е резултат на недостиг од волја, туку на недоволно јасно дефинирани улоги, канали за комуникација и процедури за координација. Како резултат, реакциите на дезинформации и наративи со потенцијал за влијание врз јавноста зависат од иницијативата на поединечни оддели или лица/поединци, наместо од системски механизам за процена и одговор.

И покрај тоа, **постои потенцијал за воспоставување функционална мрежа на институционални фокални точки, која би овозможила побрза комуникација и размена на информации при појава на информациски инцидент или криза**. Таквиот модел може да претставува преоден чекор кон воспоставувањето централизирана координација, сместена во постојните државни структури или со создавање нова институција, со јасно дефинирани протоколи и одговорности.

2.1.3. Законска и стратегиска рамка

Иако во изминатите години се направени важни чекори во насока на дефинирање на националните политики и стратегии поврзани со отпорноста на хибридните и информациските закани, правната и институционалната рамка за справување со СММИ сè уште не се целосно воспоставени. Постојат релевантни документи, пред сè Националната стратегија за градење отпорност и справување со хибридни закани (2021–2025), Националната стратегија за сајбер безбедност 2025-2028, Стратегијата за реформа на јавната администрација 2023-2030, како и активности на неколку ресорни министерства и регулаторни тела, но нивната операционализација е ограничена и меѓусебно неусогласена.

Нема јасна поделба на одговорностите во делот на превенција, следење и реакција при појава на СММИ, ниту пак механизам за координирано известување и размена на информации меѓу институциите. Како резултат, дел од мерките предвидени во Акциски план на Стратегијата за градење отпорност и справување со хибридни закани не е реализиран или се спроведува делумно, најчесто на секторско ниво.

Во однос на нормативниот аспект, постоечките закони не ги препознаваат специфичните форми на странско информациско влијание, туку се фокусираат на сродни области: медиумска регулација, сајбер безбедност, заштита на лични податоци и изборни процеси. Ова создава фрагментирана регулаторна средина, во која дел од аспектите на СММИ остануваат надвор од јасно дефинирана институционална надлежност, без носител на интегриран пристап.

И покрај тоа, постојната стратегиска рамка претставува добра основа за натамошен развој. **Потребно е поврзување на стратегиските документи и нивно ажурирање со оглед на новите предизвици, како и создавање**

единствен национален документ што би ги интегрирал аспектите на медиумска писменост, дигитална безбедност, стратегиски комуникации и превенција од странски манипулации со информации и облици на комуникациско влијание.

2.1.4. Капацитети и ресурси

Институциите задолжени за активности поврзани со СММИ се соочуваат со ограничени човечки, технички и финансиски ресурси. Во повеќето институции нема посебни одделенија или поединци со дефинирани задачи за следење и анализа на информациските влијанија, а постојните капацитети најчесто се распределени меѓу различни организациски единици.

Недостасуваат континуирана едукација за вработените во јавната администрација во доменот на медиумската и дигиталната писменост, вештини за анализа на информациите и разбирање на хибридните закани. Иако во последните години се спроведени неколку програми за обука (на пр. во рамките на НАТО, ЕУ и билатерални партнерства), тие не се систематизирани и ретко се мултисекторски.

Техничките ресурси, особено за мониторинг и анализа на онлајн содржини, се ограничени, а размената на информации меѓу институциите често се потпира на неформални контакти. Се препознава дека граѓанскиот и медиумскиот сектор располагаат со релевантни алатки и експертиза што државата би можела поефикасно да ги интегрира во заеднички напори за следење и анализа на дезинформациски кампањи.

Во овој контекст **се нагласува потребата од развивање национален систем за рано предупредување и воспоставување една референтна точка за координација на активностите поврзани со информациски манипулации, која би ги поврзувала постојните институционални и невладини ресурси**.

2.1.5. Перцепција на можностите и предлози за подобрување

И покрај воочените ограничувања, се согледуваат повеќе позитивни можности и потенцијали за унапредување на институционалниот одговор на СММИ:

- **јасно дефинирање на улогите и надлежностите преку ревидирање и ажурирање на постојните стратегиски документи и воведување оперативни протоколи за меѓуинституционална соработка;**
- **создавање формализиран координативен механизам или зајакнување на постојниот Совет за координација на безбедносно-разузнавачката заедница со конкретни задачи за следење, анализа и известување за СММИ;**
- **воспоставување систем за континуирана обука и регулирана**

размена на искуства меѓу институциите, медиумите и академската заедница;

- интеграција и унапредување на медиумската писменост и дигиталната отпорност како трајна компонента во образовните и административните програми;
- продлабочување на меѓународната соработка, особено со НАТО, ЕУ, Хибридниот центар за извонредност во Хелсинки (Hybrid CoE) и други партнерски иницијативи за борба против дезинформации;
- поддршка на партнерството со академски, граѓански и медиумски организации, како ресурс за проверка на факти и детекција на дезинформациски трендови.

2.1.6. Клучни предизвици

Врз основа на сите дискусии, се издвојуваат неколку системски предизвици што го ограничуваат капацитетот на државата за справување со СММИ.

Табела 3: Системски предизвици за одговор на СММИ

Област	Клучен предизвик
Институционална координација	Отсуство на активен координативен механизам и јасна распределба на улогите меѓу институциите.
Капацитети и ресурси	Недоволен број обучени кадри, ограничени технички алатки и слаба меѓусекторска размена.
Правна рамка	Непостоење на законска основа што директно го опфаќа СММИ; преклопување на надлежностите.
Информациска размена	Неформална комуникација и недостиг од стандарди за известување и координација.
Општествена отпорност	Недоволна медиумска писменост и ниско ниво на доверба во институциите.
Меѓународна соработка	Ограничено искористување на постојните иницијативи на НАТО, ЕУ и партнерите за борба против дезинформации.

2.2. Анализа на состојбата на системот (GAP Analysis)

Во овој дел се систематизирани критичните јазови помеѓу постојната стратегиска и правна рамка и реалната институционална практика за одговор на странското мешање и манипулирање со информации. Домените директно се пресликуваат во темите од квалитативното истражување (2.1.), за да се обезбеди чист премин од „каде сме" кон „што недостига" и подоцна кон „што треба да правиме" (глави 3 и 4). Анализата е изработена со споредување на: (а) наодите од фокус-групите и интервјуата (рутини, процеси, капацитети) и (б) постојните политики и стратегии и формалната институционална поставеност. Секој домен е оценет по три прашања: што недостига (јаз), која е последицата и која е потребната мерка.

2.2.1. Институционална поставеност и координација

Јаз	Последица	Мерка
Делумно формализирани фокални точки - офицери за комуникации, со нееднакво функционирање и нејасни линии на известување; недостасуваат унифицирани стандардно-оперативни постапки (*SOPs*) и рутини за меѓуинституционална координација за СММИ; Постојат канали за комуникација, но не се институционализирани: нема јасни постапки, рутини и одговорни носители, недоволна информираност за нивната употреба и неуедначена практична примена за редовна и структурирана размена на информации, ставови и препораки меѓу засегнатите страни;	Отежнато навремено споделување информации, заедничко планирање, носење одлуки и синхронизирано дејствување, особено во ситуации што бараат прецизна проценка на ризиците и брза реакција; Импровизација без релевантни и точни податоци и ненавремена и неефективна реакција; Ад хок реакции при закана или инцидент - различни институции реагираат одделно, без стратегија и координирана комуникација, што може да доведе до конфузија кај јавноста и намалена доверба во институциите;	Фокални точки во секоја релевантна институција, како примарни контакти во меѓуинституционалната мрежа, со јасни надлежности за координација и комуникација заради брза размена на информации, иницирање заеднички активности и навремено информирање на носителите на одлуки; Уедначено и рутинско користење на каналите и алатките за координација, со јасни носители, временски тригери и постапки за редовно и итно информирање и упатување кон релевантните институции;

Не се развиени јасни постапки (*SOPs*) за постапување во различни сценарија, случаи на ескалација или кризни ситуации; Ретки и нерегулирани кратки ситуациски брифинзи, за да се обезбеди консолидирана и ажурирана слика за тековните состојби.	Удвојување на напорите без јасно распределени надлежности - различни институции може да преземаат слични активности без да бидат свесни за тоа, што троши ресурси и го отежнува процесот на анализа и носење одлуки; Неусогласени пораки кон јавноста што се клучни за управување со јавната перцепција и одржување на социјалната стабилност.	Стандардно-оперативни постапки за идентификување инциденти, нивна процена според однапред утврдени критериуми и координиран институционален одговор за различни типови ситуации (чекори за внатрешна комуникација, активирање на фокалните точки, информирање на јавноста и ескалација кон повисоки нивоа на одлучување); Редовни ситуациски брифинзи меѓу институциите за проценки на тековните ризици, анализи на претходни инциденти и препораки за подобрување на координацијата.

2.2.2. Стратегиска рамка (операционализација)

Јаз	Последица	Мерка
Постојат стратегии, но оперативната рамка за СММИ е недоволна: нема заеднички работен поим, улогите и надлежностите се непрецизни, а постапките ретко се сведени на протоколи и индикатори.	Неизвесност „кој води“ при инцидент, преклопување на надлежностите и бавни одлуки; Ризик од прекумерна регулација поради нејасни процеси.	Оперативна рамка (работна дефиниција, мапа на улогите и одговорностите, листи за проверка и сценарија, шаблони за одлуки и јавни пораки), поткрепена со подзаконски акти и упатства, наместо веднаш нов закон.

2.2.3. Капацитети и ресурси

Јаз	Последица	Мерка
Ограничен кадар во клучните профили (OSINT, податочна аналитика, стратегиска комуникација); Недостиг од заеднички алатки за мониторинг и анализа; Отсутна политика за институционална меморија.	Зависност од поединци; Нерамномерно покривање на ризиците, бавна детекција и слаб квалитет на анализите; недостиг од институционална меморија.	План за обуки по нивоа (основно–напредно–специјализирано); Организирање редовни тренинзи за кризна комуникација за да се обезбеди конзистентност и кредибилитет во јавните пораки; Институционализирање на централен „сет од алатки" со техничка поддршка и лиценци; Формализирани практики за пренос и задржување на знаењето (предавања, бази на знаење, менторство).

2.2.4. Стандарди за размена на информации

Јаз	Последица	Мерка
Размената на информации најчесто е неформална; Нема стандарден шаблон за инциденти (минимум полиња и метаподатоци); Нема централен репозиториум.	Делумна слика и губење податоци; Паралелни верзии на исти анализи; Задоцнет заеднички одговор.	Стандарден шаблон за пријава и следење инциденти; Заеднички репозиториум со контроли на пристап за размена на информации; Именуван национален контакт за Системот за брзо предупредување на ЕУ (RAS) (каде што е применливо).

2.2.5. Комуникациска отпорност и писменост

Јаз	Последица	Мерка
Недостасува систематска превентивна (prebunking) и корективна (debunking) комуникација, како и заеднички насоки за транспарентност; Ниска медиумска и дигитална писменост во јавниот сектор.	Празнина во јавната расправа што лесно се пополнува со манипулативни наративи; Пад на довербата и поголема ранливост.	Кратки комуникациски стандардно-оперативни постапки (кој, кога, како порака); Превентивни пораки за очекувани наративи (пред избори или кризи); Програми за медиумска и дигитална писменост и формализирани партнерства со академија, граѓански организации и медиуми.

2.2.6. Мониторинг и евалуација

Јаз	Последица	Мерка
Недостига сет од клучни индикатори за перформансите и рутината за месечното или кварталното известување; Мерките ретко се следат преку резултати.	Тешко се мери ефектот; Ограничено институционално учење и слабо аргументирање за потребните ресурси.	Пакет со клучни индикатори за перформансите по домени (координација, капацитети, одговор, комуникација); Квартални брифови, годишен извештај и ревизија на мерките.

ГЛАВА 3:

КОМПАРАТИВНИ ИСКУСТВА И МОДЕЛИ ЗА ОДГОВОР НА СММИ

Компаративната анализа на различни национални пристапи овозможува да се идентификуваат добрите практики, слабостите и потенцијалите за приспособување во локален контекст. Табеларниот приказ систематизира институционални решенија што различни држави ги применуваат за справување со странското мешање и манипулирање со информации. Преку споредба на законските рамки, оперативните механизми, улогата на безбедносните служби, независните тела и граѓанското општество, се добива појасна слика за тоа кои модели се покажале ефективни, а кои се соочуваат со структурни или политички ограничувања.

Освен тоа, оваа анализа овозможува критичко разгледување на степенот на интеграција меѓу различни институции – од разузнавачки служби до медиумски регулатори, и нивната способност за координирано дејствување. Во услови на брзо менување на природата на заканите, клучни се флексибилноста и интердисциплинарниот пристап. Затоа, табеларната презентација не само што служи како аналитичка алатка, туку и како практичен ресурс за креирање препораки за институционална рамка применлива за Северна Македонија.

Табела 4: Систематизиран приказ на националните модели за одговор на СММИ

Земја/ организација	Институција / модел	Тип на структура	Клучни функции	Извор
Франција	VIGINUM	Јавна служба под премиерот	OSINT, анализа на дигитални влијанија, интерминистерска координација	https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
Германија	FIMI-ISAC	Мрежа на организации (неформална)	Споделување информации, поддршка на изборните тела, медиумите и граѓанскиот сектор	https://neweasterneurope.eu/state-responses-to-fimi-and-recommendations-for-resilience/
Шведска	Агенција за психолошка одбрана	Независна владина агенција	Мониторинг, едукација, поддршка на медиумите и јавните институции	https://cospr.org/evolving-threat-of-foreign-information-manipulation-and-interference-fimi-critical-insights-from-3rd-eeas-report/
Финска	Национална стратегија за медиумска писменост	Образовен и владино-институционален модел	Образование, јавни кампањи, истражувања	https://www.europarl.europa.eu/RegData/etudes/TUD/2021/653632/EXPO_STU%282021%29653632_EN.pdf

Естонија	Центар за стратегиска комуникација	Владина канцеларија	Превенција од дезинформации, медиумска писменост, дигитална отпорност	https://www.hybrid-coe.fi/
Литванија	Целосна стратегија за одбрана, МВР, единици за стратегиска комуникација	Модел на сеопфатен владин (whole-of-government) и сеопфатен општествен (whole-of-society) пристап	Цивилна и информациска отпорност, стратегиски комуникации, сајбер одбрана, отпорност на информации, стратегиска комуникација, сајбер одбрана	https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323902/lithuanias-total-defense-review/
Полска	Совет за отпорност, INFO OPS Polska, FIMI-ISAC (Изборен интегритет)	Координација меѓу повеќе актери (влада + граѓанско општество)	Заштита на изборите, јавна свест, известувања за инциденти, стратегиска координација	https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/
Чешка	Владина координација за стратегиски прашања, BIS, FIMI-ISAC	Владина координација плус безбедносна заедница	Сајбер безбедност, дезинформации, избори, мониторинг, образование	https://www.informed-society.cz/wp-content/uploads/2024/10/EN_Safeguarding_Democracy_2024-09-26.pdf
Словачка	Центар за спротивставување на хибридни закани (CCHT)	Единица при МВР	Мониторинг, стратегиски комуникации, образование, ажурирање на регулативите	https://www.hybrid-nehrozby.sk/ccht/
Украина	Центри за стратегиска комуникација	Владина и воена структура	Контрапропаганда, анализа на влијанија, меѓународна соработка	https://www.hybrid-coe.fi/
Романија	Национални иницијативи за изборна заштита и мониторинг со ВИ	Владина стратегија + регулаторни тела	Мониторинг на Тикток, манипулации со ВИ, изборна безбедност	https://visegradinsight.eu/safeguarding-democracy-against-information-manipulation-and-hybrid-threats/

Црна Гора	Министерство за надворешни работи (Меморандум за разбирање со САД), CDT, Медиумска стратегија 2023–2027	Владина координација и граѓанско општество	Дезинформации, мониторинг, законодавна реформа, транспарентност, заштита на изборните процеси	https://www.gov.me/en/article/memorandum-of-understanding-signed-between-the-ministry-of-foreign-affairs-of-montenegro-and-the-us-department-of-state-close-cooperation-for-more-effective-fight-against-disinformation
ЕУ	EEAS / EUvsDisinfo	Паневропска институција	Архива на дезинформации, дипломатски одговори, санкции	https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
НАТО	Тимови за поддршка против хибридни напади	Мултинационална платформа	Поддршка на земји членки, анализа, стратегиска комуникација	https://www.nato.int/cps/en/natohq/topics_156338.htm
САД	Глобален центар за ангажман (GEC)	Меѓуагенциска платформа	Анализа, партнерства, стратегиска комуникација	https://govfacts.org/federal/eop/how-the-national-security-council-fights-foreign-disinformation-campaigns/
Канада	Механизам за брза реакција (RRM)	Владина платформа + Г7 координација	Мониторинг, јавна едукација, меѓународна координација	https://2021-2025.state.gov/the-framework-to-counter-foreign-state-information-manipulation/
Тајван	Национални програми за дигитална отпорност	Владина стратегија + граѓански сектор	Технолошки решенија, едукација, изборна заштита	https://neweasterneurope.eu/state-responses-to-fimi-and-recommendations-for-resilience/

Подолу следуваат пет модели што, иако различни по институционална форма, споделуваат заеднички карактеристики: централен/јадрен капацитет, мрежа на фокални точки, протоколи (*SOPs*), редовна процена на ризици и вградена јавна комуникација.

3.1. Естонија: дигитална држава со рутини за свесност и координација

Естонија ја темели институционалната отпорност врз пристапот за јавната администрација „дигитално како стандард" (*digital-by-default*), во која управувањето со (мета)податоците и пристапите до нив е стандарден дел од секојдневната работа. Одговорот на информациските закани се врши преку Центарот за стратегиска комуникација при Владата и е ритуализиран: кратки, фиксирани ситуациски брифинзи (1–2 страници) што редовно се подготвуваат и се распределуваат; фокални точки во министерствата, агенциите и клучната инфраструктура што имаат јасни должности за известување и ескалација; и симулациски вежби на маса (*table-top - TTX*) што се одржуваат годишно, често пред чувствителни периоди (избори, геополитички тензии и сл.).

Процесите се потпираат на стандардизирани формати: шаблони за инциденти со минимум полиња (датум/време, извор, опис, веројатност/влијание, преземени мерки), заеднички речник на термини и минимални технички метаподатоци.

Важна особеност е спојувањето на техничките и комуникациските функции: тимови за ИКТ/сајбер и за јавна комуникација редовно седат на иста маса, што го намалува јазот меѓу техничките наоди и индикатори и усогласената комуникациска порака и соопштение.

Силни страни	Слаби страни/ризици
Дисциплина во рутините, интероперабилност, брза размена.	Висока зависност од дигиталните системи; потреба постојано да се одржуваат стандардите и да се планираат инвестициски и оперативни трошоци (CAPEX / OPEX) за алатки и одржување.

3.2. Франција (Viginum): јадрен владин капацитет против дигитални вмешувања

Вигинум (Viginum) е пример за централизиран оперативен капацитет вграден во владината архитектура. Тимот е мал, професионализиран и работи по јасен мандат: набљудување на дигиталниот простор за откривање странски вмешувања, аналитичка синтеза и алармирање кон ресорните линии кога ќе се исполни некој критериум (изборни или кризни периоди, значајно влијание).

Се работи според строг протокол: нивоа на сигнал (индикативно значајно критично), временски прозорци за известување, матрици на одговорни носители и формати за материјали „готови за употреба" (прашања и одговори, листи со факти, линија на порака). Принципот е да се обезбеди интероперабилност со различни министерства и регулатори без да се создава паралелна хиерархија. Во однос на транспарентноста, моделот практикува „минимално неопходно" јавно информирање, доволно да се посочи на ризикот без да се амплифицира наративот.

Силни страни	Слаби страни/ризици
Јасен мандат, брза линија „сигнал одлука порака".	Централизацијата бара константна меѓуресорска доверба; претераната јавна изложеност може да отвори непотребни полемики.

3.3. Полска: интерсекторска процена на ризиците и квартални брифинзи

Полскиот модел ги поставува процените на ризик како мотор на координацијата. Безбедносните служби, ИКТ-одделите и комуникациските тимови редовно ги вкрстуваат наодите и ги претвораат во ризик-матрици (веројатност x влијание), со кратки мерки за ублажување и носители. Овие матрици не се административен вишок, туку работна алатка за квартални брифинзи, каде што се донесуваат мали, но континуирани корекции: ажурирање на стандардно-оперативни постапки при различни сценарија, планирање вежби, усогласување пораки.

Важен елемент е каналот кон меѓудржавна координација: кога случајот има прекугранични импликации, постои навика да се вклучи Системот за брзо предупредување (*RAS*), не за префрлање на одговорноста, туку за координација на информациите и временските прозорци на реакција.

Силни страни	Слаби страни/ризици
Предвидлив ритам и култура на заедничка процена; лесна преносливост на форматот.	Опасност од пристап „само да се обележи како завршено" ако брифинзите се сведат само на формалност; потребно е лидерство што инсистира на применливи резултати.

3.4. Шведска: Агенција за психолошка одбрана

Шведската агенција за психолошка одбрана го институционализира јакнењето на општествената отпорност преку обуки, советување и оперативна поддршка. Поставеноста е хоризонтална: Агенцијата не е центар за демантирање, туку помага да се зголеми капацитетот, кој им помага на ресорните институции да комуницираат со јавноста во сложени ситуации (од влијателни операции до кризни настани).

Клучни практики се каталозите на обуки (од основни до специјализирани модули за комуникациски тимови, аналитичари, менаџери), насоки за јавна комуникација во изборни и кризни периоди (формулирање пораки без амплификација, работа со медиуми, визуелни стандарди) и прегледи по настан (after-action review) што обезбедуваат институционална меморија и учење.

Силни страни	Слаби страни/ризици
Стабилен фокус на компетенциите и долгорочно учење; доверба кај јавноста поради советодавната (не полициска) улога.	Успехот зависи од доброволноста и отвореноста на ресорните институции; потребни се јасни критериуми за приоритети.

3.5. Финска: писменост, партнерства и превентивни комуникации

Финска ја третира информациската средина како јавен капацитет и инвестира во програми за медиумска и информациска писменост за јавната администрација, наставниците, учениците, новинарите и локалните заедници. Паралелно, се развиваат превентивни комуникации (*prebunking*): кратки, повторливи циклуси на пораки насочени кон очекувани наративи пред избори, референдуми или кризни настани.

Методолошки, финскиот пристап се потпира на кодизајн со јавниот сервис, академскиот и граѓанскиот сектор, што ги зголемува легитимноста и опфатот. Пораките се тестираат на јасност и доверба, наместо само на досег, и редовно се мерат индикаторите како разбирање, доверба и „време до исправка". Ова создава култура во која јавните институции поседуваат комуникациска компетенција, а не се потпираат исклучиво на итна исправка во криза.

Силни страни	Слаби страни/ризици
Висока социјална легитимност и партнерства; мерливост на ефектите.	Побавен циклус на резултати; потребна е долгорочна поддршка и политички консензус за програмите.

ГЛАВА 4:

ОПЦИИ ЗА ПОЛИТИКА ЗА ОДГОВОР НА СММИ ВО СЕВЕРНА МАКЕДОНИЈА

Оваа глава нуди три реалистични архитектури за системски одговор на СММИ. Намерата е да се постави јасен избор меѓу различни патишта, секој со препознатливи функции, предности и ограничувања.

4.1. Опција А: Самостоен центар за национална отпорност

Управувачка поставеност

Самостоен јавен субјект (агенција, центар) основан со посебен акт, со сопствен буџет и јасно дефиниран мандат. Центарот е независен во аналитичката работа, но одговорен за координација со ресорните институции преку формализирани механизми (меморандуми, правилници). Транспарентност и усогласеност со националните стратегии обезбедува надзорна или советодавна комисија.

Клучни функции:

- национално набљудување и анализа на информативната средина (СММИ), вклучително трендови, наративи и техники;
- координација на институциите преку мрежа на фокални точки и редовни брифинзи;
- стандарди за размена на информации и централен репозиториум (формати, метаподатоци, нивоа на доверливост);
- каталог и спроведување обуки (основни–напредни–специјализирани);
- поддршка за институционална комуникација (претходно откривање закани *[prebunking]* и разоткривање инциденти *[debunking]*, прашања и одговори, листи со факти);
- логика на мониторинг и евалуација (индикатори за успешност, квартални и годишни извештаи).

Процеси и стандардно-оперативни процедури

Центарот усвојува „минимален сет" на стандардно-оперативни процедури: пријава–процена–одговор (со временски прозорци), матрица на носители на одлука, нивоа на алармирање и шаблони за ситуации (избори, кризи, чувствителни настани). Вграден е циклус на редовни ситуациски брифови (месечни) и тематски аналитички белешки.

Ресурси и кадар

Јадро од 15–25 професионалци (OSINT/податочна аналитика, сајбер/технички профили, стратегиски комуникации, правник за регулаторни прашања, мониторинг и евалуација). Централен сет алатки за мониторинг и аналитика, со заеднички лиценци и техничка поддршка.

Односи со јавноста и комуникација

Не претставува центар за деманти, туку сервис за носителите на пораки (министерства и агенции): подготвува комуникациски препораки, координира превентивни пораки пред чувствителни периоди и обезбедува материјали за непосредна примена.

Меѓународна соработка

Официјален контакт со европските механизми (на пример, *RAS*) и со тематски центри (на пример, Hybrid CoE), учество во обуки и симулациски вежби и споделување стандарди.

Предности

Јасен институционален идентитет; централизирана експертиза и алатки; стабилна институционална меморија; висока отчетност и видливост.

Ограничувања

Потреба од нова правна рамка и буџет; ризик од удвојување ако не се прецизираат улогите; потребно време за кадровско зајакнување и процедури.

4.2. Опција Б: Национален координативен механизам под Владата

Управувачка поставеност

Координативна канцеларија вградена во Владата (под премиер, генерален секретаријат или сл.), која функционира како „јадро + мрежа". Јадрото координира, а ресорите носат и спроведуваат. Политичката вертикала овозможува брза ескалација и синхронизација меѓу министерствата и агенциите.

Клучни функции

- Организирање месечни ситуациски брифинзи и квартални процени на ризиците (веројатност x влијание). За структурирање на проценките се практични рамките PMESII и AIC (US Army, 2015).

- Договорен стандарден шаблон за пријавување и следење инциденти и меѓуресорен репозиториум (може технички да го хостира постојна институција).
- Усогласување на јавната комуникација (насоки, прашања и одговори, листи со факти).
- Координирање на каталог на обуки (спроведување преку ресори и партнери).
- Поврзување со механизмите на НАТО и ЕУ.

Процеси и стандардно-оперативни процедури

Основата се „едноставни, но обврзувачки" стандардно-оперативни процедури за пријава – процена – одговор: јасни чекори и временски рокови; матрица на носители; скала за ескалација (кој-кому-кога). Внатрешниот календар создава ритам (месечно на техничко ниво, квартално на повисоко ниво).

Ресурси и кадар

Јадрото има 8-12 лица (координатори, аналитичари, специјалисти за комуникации, правник и координатор за мониторинг и евалуација). Алатките за мониторинг и анализа се обезбедуваат преку рамковни договори и лиценци и се користат преку постојните платформи и капацитети на институциите, без удвојување на инфраструктурата.

Односи со јавноста и комуникација

Координацијата на пораки е поддржувачка функција: усогласени насоки за комуникација, календар на овластени говорници и кратки превентивни брифови пред чувствителни теми. Јавната видливост е умерена, бидејќи главниот акцент е на навремената внатрешна координација и обезбедувањето листи со факти, прашања и одговори што ресорите можат веднаш да ги користат. Онлајн каналите овозможуваат 'конективна акција' и брза мобилизација на публики (Bennett & Segerberg, 2012).

Меѓународна соработка

Владината канцеларија дејствува како единствена контакт-точка кон RAS, EEAS и партнерските влади, што овозможува брза и формална размена на информации, навремено учество во предупредувања и вклучување во заеднички анализи и вежби.

Предности

Брз старт без нова институција; силна меѓуресорска тежина; минимален институционален отпечаток; лесно усогласување со постојните ресурси.

Ограничувања

Зависност од стабилност на политичкото раководство и приоритетите; ризик аналитичката длабочина да биде ограничена ако јадрото е премало; видливоста кон јавноста и академската заедница може да биде пониска.

4.3. Опција B: Зајакнување на постојниот Совет за координација на безбедносно-разузнавачката заедница

Управувачка поставеност

Потпирање на постојниот Совет за координација на безбедносно-разузнавачката заедница, со јасно додаден мандат за СММИ. Се создава „секретаријатско јадро", кое обезбедува процеси, документација и аналитичка поддршка, а ресорите остануваат примарни носители.

Клучни функции

- Календар на рутински состаноци (месечно на техничко ниво, квартално на раководно ниво).
- Усвојување стандардно-оперативни процедури со сценарија, листи за проверка и јасни ескалациски канали.
- Заеднички репозиториум и стандарден формат за инциденти и анализи.
- Внатрешна линија за комуникација: јасна патека „кој пишува - кој проверува - кој одобрува - кој објавува", со шаблони за прашања и одговори и именувани портпароли, а по потреба се координира со ресорните носители.
- Вклучување во европските механизми преку именувани фокални точки.

Процеси и стандардно-оперативни процедури

Фокусот е на „оживување" на координацијата: редовни брифинзи, документирани одлуки и следење на извршувањето. Рутините и „внимателното организирање" ја зголемуваат организациската сигурност и отпорност (Weick & Sutcliffe, 2007). Стандардно-оперативните процедури мора да се конкретни (кој, што, кога), со кратки индикатори за статусот.

Ресурси и кадар

Секретаријатско јадро од 5-8 лица со процесна и аналитичка компетенција, мрежа на фокални точки во релевантните институции и користење на постојните алатки и инфраструктура без удвојување. Инвестициите во човечки капацитети, процеси и инфраструктура се предуслов за одржливост (UNDP, 2021).

Односи со јавноста и комуникација

Советот традиционално функционира како интерно координациско тело, а јавната комуникација се реализира преку ресорните институции. Потребни се јасни правила кога и како се излегува со усогласени пораки и кој е овластен говорник во

конкретни ситуации. Поголемата транспарентност е поврзана со повисока доверба во институциите (Grimmelikhuijsen et al., 2013).

Меѓународна соработка

Контактите со надворешни партнери се одржуваат преку ресорите и преку именувани фокални точки, а секретаријатот ги координира документите, форматите и роковите.

Предности

Најниска институционална цена; искористување на постојната архитектура и доверливи канали; релативно брзо операционализирање.

Ограничувања

Пониска јавна видливост; ризик координацијата да остане формална без реална примена; зависност од дисциплината и стабилноста на лидерството во Советот.

Табела 5: Опции за архитектури за системски одговор на СММИ

Критериум	**Опција А: Самостоен центар**	**Опција Б: Координативен механизам при Владата**	**Опција В: Зајакнат Совет за координација на безбедносно-разузнавачката заедница**
Управувачка поставеност	Самостоен јавен субјект (агенција/центар) со сопствен буџет и надзорна/советодавна комисија.	Координативна канцеларија под премиер/Генерален секретаријат („јадро + мрежа").	Постоечки Совет со секретаријатско јадро и проширен мандат.
Мандат и функции	Набљудување и анализа на СММИ; координација преку фокални точки; стандарди и репозиториум; обуки; комуникациска поддршка; мониторинг и евалуација; ЕУ/НАТО врски.	Рутинска координација; месечни брифинзи и квартални процени; стандарден шаблон и споделување; усогласена јавна комуникација; каталог на обуки; ЕУ/НАТО врски.	Редовни состаноци (техничко/раководно ниво); стандардно-оперативни процедури со сценарија; заеднички репозиториум; внатрешни линии за комуникација; ЕУ контакти преку фокални точки.

Критериум	Опција А: Самостоен центар	Опција Б: Координативен механизам при Владата	Опција В: Зајакнат Совет за координација на безбедносно-разузнавачката заедница
Процеси / СОП	Формализирани стандардно-оперативни процедури (пријава–процена–одговор); нивоа на алармирање; шаблони за ситуации; месечни брифинзи.	„Лесни“, но обврзувачки стандардно-оперативни процедури; календар (месечно/квартално); ескалациски канали.	Оживување на координацијата: конкретни стандардно-оперативни процедури; листи за проверка; документирани одлуки и следење.
Кадар (ориентир)	Јадро 15–25 (OSINT/аналитика, сајбер/технички, комуникации, право, мониторинг и евалуација).	Јадро 8–12 (координација, аналитика, комуникации, право, мониторинг и евалуација).	Секретаријат 5–8 + фокални точки во институции.
Алатки/ репозиториум	Централен сет на алатки и хостиран национален репозиториум со стандарди за метаподатоци.	Координиран пристап (рамковни договори/ лиценци); репозиториум хостиран кај постојна институција.	Користење на постојните алатки; договорен репозиториум и формат.
Комуникација со јавност	Подготвува препораки/ материјали „готови за употреба“; поддржува носители на порака.	Усогласува пораки и распоред на носители; средна јавна видливост.	Главно внатрешна координација; јавната комуникација преку ресорите.
Меѓународна соработка	Формален интерфејс кон ЕУ и НАТО механизмите; учество во обуки и специјализирани вежби.	Природен владин интерфејс кон ЕУ/ НАТО механизми; брза формална комуникација.	Контакти преку ресорите и именувани точки; координација преку секретаријат.
Предности (резиме)	Јасен идентитет; централизирана експертиза; стабилност и висока отчетност.	Брз старт; силна меѓуресорска тежина; минимален институционален отпечаток.	Најниска институционална цена; користи постоечки канали; брза оперативизација.

Критериум	Опција А: Самостоен центар	Опција Б: Координативен механизам при Владата	Опција В: Зајакнат Совет за координација на безбедносно-разузнавачката заедница
Ограничувања (резиме)	Потребни нови правни/ буџетски рамки и разграничување на улогите.	Зависност од политичкиот континуитет; ризик од плитка аналитика ако е „тенко“ јадрото.	Историска инерција; пониска јавна видливост; успехот зависи од дисциплината.
Време до оперативност	Подолг рок (потребни дизајн и формирање пред старт).	Краток рок (оперативно за неколку месеци).	Краток–среден рок (реформа на постојното и воспоставување рутини).

ГЛАВА 5:

ЗАКЛУЧНИ СОГЛЕДУВАЊА И ПРЕПОРАКИ ЗА ИМПЛЕМЕНТАЦИЈА

5.1. Заклучни согледувања

Северна Македонија, како земја со стратегиска геополитичка позиција, членка на НАТО и јасно изразени амбиции за интеграција во ЕУ, се наоѓа на точка кога мора да го развие националниот одговор на странското мешање и манипулирање со информации во сеопфатна и координирана рамка. Градењето општествена и институционална отпорност не може да се постигне со изолирани активности, туку со поставување интегриран систем заснован на стратегиско унапредување, институционална координација, едукација, јавна свест и меѓународна соработка.

Потребни се **ревизија и надградба на Националната стратегија за отпорност од хибридни закани**, која треба да се темели на современи анализи и нови типологии на закани, како што се когнитивните операции и алгоритамско влијание. Стратегијата мора да биде жив документ што ќе се приспособува на променливата безбедносна средина преку вграден механизам за следење и евалуација, кој ќе овозможи динамична адаптација на политиките. Покрај тоа, законската интервенција е суштинска. **Правното дефинирање на СММИ** е предуслов за ефикасна институционална координација и одговорност. За да се овозможи информирано одлучување, потребно е да се воспостават **алатки за проценка** што ќе користат модели применливи за анализа на хибридните закани и процена на ризиците во оперативната средина.

Отпорноста кон СММИ зависи од **постоењето на национален координативен механизам**, кој ќе овозможи редовна размена на информации, заедничка процена и усогласен одговор. За да се постигне тоа, потребно е **јакнење на институционалните капацитети** преку инвестирање во човечки ресурси, дигитална инфраструктура и аналитички технологии. Истовремено, државата мора да изгради **институционална меморија**, односно систем за архивирање, анализа и учење од претходните случаи, кој ќе спречи повторување на пропустите и ќе ја зголеми превенцијата. **Вклучувањето на граѓанското општество, академската заедница и медиумите** во процесите ќе овозможи создавање потранспарентен, инклузивен и одржлив систем на отпорност.

Образованието и медиумската писменост исто така имаат централна улога во градењето отпорно општество. Потребно е **унапредување на националните програми за медиумска и дигитална** писменост што ќе ги опфатат сите возрасни категории и ќе се интегрираат во формалното и неформалното образование. Покрај тоа, неопходни се **специјализирани обуки за јавната администрација и медиумските професионалци** што ќе ги зајакнат капацитетите за препознавање, анализирање и соодветно реагирање на информациските манипулации.

Градењето општествена отпорност бара вклученост и на граѓаните. **Систематските информативни и едукативни кампањи** се клучен инструмент за јакнење на критичкото размислување и препознавање на дезинформациите. Во тој процес,

транспарентната и отчетна институционална комуникација претставува темел на довербата меѓу институциите и граѓаните.

Конечно, **регионалната и меѓународната соработка** се предуслов за ефективен одговор на СММИ. За навремено препознавање и неутрализирање на странските влијанија особено е значајна **интеграцијата во европските механизми** Сет на алатки за одговор на СММИ (*FIMI Toolbox*) и Систем за брзо предупредување (*Rapid Alert System - RAS*), развиени од Европската служба за надворешно дејствување (EEAS).

5.2. Препораки за имплементација

За Северна Македонија да ја трансформира својата институционална архитектура за интегриран одговор што не само што реагира на заканите, туку и ги предвидува, ги анализира и ги спречува, овој документ за јавни политики препорачува **три опции за политика: (1) Самостоен центар за национална отпорност, (2) Национален координативен механизам под Владата или (3) Зајакнат Совет за координација на безбедносно-разузнавачката заедница.** Пристапот предвидува стабилно градење рутини што ќе останат и по сменувањето на раководства и приоритетите, а намерата е системот да работи и во вообичаени околности, а не само во криза.

Независно од изборот на институционалниот модел, овој документ ги предвидува следните **препораки или патоказ за имплементација**:

- **Да се обезбеди јасен носител на процесот и формален легитимитет.** Без оглед дали тоа ќе биде самостоен центар, владин координативен механизам или зајакнат совет, мандатот треба да биде експлицитно опишан на кратко: со наведени цели, опсег, одговорности и јасни канали и правила за соработка со клучните институции.

- **Секоја релевантна институција да номинира фокална точка и заменик**, со една страница опис на улогата, чекорите кога и кому му се проследуваат случајот и обврските за редовно известување.

- **Да се утврди календар на рутини** откако ќе се воспостави оваа минимална инфраструктура, и тоа: кратки технички состаноци со ситуациски бриф еднаш месечно и покомпактни состаноци на повисоко ниво еднаш квартално, на кои се носат насоки, се следат решенија и се коригира курсот таму каде што е потребно. За да не се изгуби ништо во оперативната брзина, по секој состанок се подготвува краток запис за одлуките за тоа што е одлучено, кој е одговорен и што следува.

- **Да се дефинира главната постапка на „пријава–процена–одговор“**. Таа се утврдува со јасен документ што наведува: кои информации се пријавуваат, во

кој минимален формат, кому му се доставуваат и во кој рок; како се врши процена на ризикот (едноставна матрица: веројатност х влијание); и како се носи одлука за одговор, со јасно определени одговорности и временски прагови. Оваа логика се надополнува со неколку универзални сценарија (изборен период, кризни состојби, чувствителни настани), за кои однапред се подготвуваат листи за проверка, носители и формат на излезните материјали. Јасното дефинирање кога и кому се проследува случајот се подига на повисоко ниво. На една страница се утврдува: кој одлучува на техничко ниво, кога се вклучува политичкиот носител и во кој момент јавноста се информира. Овие прагови ја прават постапката предвидлива и правична.

- **Да се развиваат институционалните компетенции**. Во „јадрото" на системот се потребни најмалку три вида профили: аналитика и отворени извори (со податочна писменост), ИКТ/сајбер врска со способност да преведе технички сигнал во оперативно разбирлива порака и стратегиска комуникација за формулирање точни, јасни и доверливи комуникациски материјали. На ова се надоврзуваат правничката поддршка за регулаторните прашања и координацијата за мониторинг и евалуација, дури и ако некои од тие улоги се споделени. Овој кадровски профил има смисла само ако е поддржан од заеднички сет алатки за мониторинг и анализа и од едноставна, стабилна инфраструктура за евиденција на случаи.

- **Да се креира каталог на обуки** на три нивоа: основни модули за сите фокални точки, напредни за аналитичарите и комуникаторите и специјализирани за изборни и кризни сценарија. Секоја обука треба да има јасна цел, временска рамка и видлив резултат (алатка или документ за употреба), со официјална потврда за завршена обука што ќе ја задржи институционалната меморија дури и при ротации на кадарот.

- **Да се подготвуваат кратки, разбирливи пораки за очекуваните наративи** уште пред да се појават во чувствителни периоди. Наместо да се чека демант, комуникацијата со јавноста заслужува посебен, превентивен третман. Овие објаснувања за претходно разоткривање на заканите (*prebunking*) не се пропаганда, туку сервис за граѓаните: што е факт, што е шпекулација и каде да се проверат информациите. Кога корекцијата е неопходна, се користат стандарден формат на прашања и одговори и листи со факти што можат брзо да ги преземат институциите носители. Важно е правилото на „минимално неопходна" изложеност: јавноста треба да биде информирана, но без непотребно амплифицирање на манипулативните наративи. За ова да функционира, треба да постои ажурирана листа на контакти и јасен протокол за работа со медиумите и платформите, со насоки за транспарентност и временска координација.

- **Да се стандардизира размената на информации** за намалување на шумот и забрзување на одлуките. Секој инцидент или релевантно набљудување се евидентира со минимален, но задолжителен сет на полиња: датум и време, извор или линк, краток опис, проценка на веројатноста и влијанието, преземените мерки и моменталниот статус. Овие записи се чуваат во заедничка, контролирана локација со верзионирање и основни метаподатоци; не е пресудно каде е хостиран

репозиториумот, туку да е стабилен, доследен и да има јасни нивоа на пристап. Кога случајот има прекугранична димензија, внатрешниот протокол треба да наведува кој и кога иницира активирање на европските канали, особено Системот за брзо предупредување (*RAS*), со што националниот напор станува дел од поширока координација.

- **Да се воспостави минимална мерливост** за системот да учи. Нема потреба од комплексни индикаторски рамки; доволно е по еден мал сет на индикатори во секој домен: редовност и квалитет на брифинзите и состаноците; број и покриеност на обучените фокални точки; времето од сигналот до првата координирана порака; досегот и разбирливоста на комуникациите; и процентот на записите што пристигнуваат во стандарден формат. Овие показатели се консолидираат во краток месечен ситуациски бриф и квартален преглед, во кој секогаш има место за две-три конкретни корективни мерки. Воспоставувањето систем на научени лекции ја храни институционалната меморија и ја намалува зависноста од поединци.

Овој патоказ ја поставува минималната, но клучна инфраструктура: јасен носител, мрежа на фокални точки за контакт, практични постапки, јадрени компетенции, предвидлива комуникација и мерливост што поттикнува учење. Така, без разлика дали ќе се избере самостоен центар, владин координативен механизам или реформиран совет, системот добива „ритам“, кој ја претвора добрата намера во секојдневна практика.

ЗА АВТОРИТЕ

Д-р Александар Грижев е вонреден професор на Воената академија „Генерал Михаило Апостолски" – Скопје и раководител на Катедрата за општествени и хуманистички науки. Неговиот наставно-истражувачки фокус е на безбедносно-одбранбените студии, постконфликтната стабилизација и реконструкција, реформите на безбедносниот сектор (*SSR*), радикализација и насилен екстремизам, когнитивни операции и родова перспектива во вооружените сили и поширокиот безбедносен сектор. Има оперативно искуство од меѓународни мисии, вклучително и учество во Специјалната мониторинг мисија на ОБСЕ во Украина (2019–2021), како и претходни ангажмани во конфликтни и постконфликтни средини. Редовно учествува на меѓународни форуми и е дел од различни проекти и активности со национални и меѓународни партнери (*NATO Science and Technology Organization, NATO Committee on Gender Perspective, OSCE, UN, RACVIAC, PfP Consortium*). Со посебен интерес во културните и религиозните димензии во операциите, го истражува градењето институционална отпорност кон хибридните закани, со посебен фокус на странското мешање и манипулирање со информации (СММИ), институционална координација, јавна отпорност на манипулативни наративи и етичка комуникација во безбедносниот сектор.

Д-р Весна Попоска е универзитетска професорка, независна аналитичарка и единствената жена со одбранет докторат на Воената академија „Генерал Михаило Апостолски" во Скопје - подвиг што ја позиционира како пионерка во безбедносните и одбранбените студии во Северна Македонија. Нејзината експертиза опфаќа прашања од областа на националната безбедност, хибридните закани, демократската отпорност и правната рамка на одбранбените политики. Попоска ги има посетувано Школата за политика на Советот на Европа, Претседателската школа за млади лидери и Варшавскиот безбедносен форум - три престижни платформи што ја обликуваат нејзината стратегиска перспектива и ја поврзуваат со водечките европски и глобални безбедносни мрежи. Таа е надворешна истражувачка на Институтот Преспа, каде што работи на проекти поврзани со демократијата, човековите права и регионалната стабилност, со посебен акцент на отпорноста на институциите кон хибридни влијанија. Како вонредна професорка на Воената академија во Скопје, активно придонесува кон развојот на современи наставни програми во областа на безбедноста и одбраната, со фокус на хибридните закани, стратегиската комуникација и градењето институционална отпорност. Нејзиниот академски ангажман е проследен со многубројни јавни настапи, панел-дискусии и публикации. Весна Попоска е гласна поддржувачка на родовата еднаквост во безбедносниот сектор и се залага за поголема вклученост на жените во процесите на одлучување и креирање политики.

КОРИСТЕНА ЛИТЕРАТУРА

- Banas, J.A. & Miller, G., 2013. *Inducing resistance to conspiracy theory propaganda: Testing inoculation and metainoculation strategies. Human Communication Research*, 39(2), pp.184–207.
- Bennett, W.L. & Segerberg, A., 2012. The logic of connective action. Information, Communication & Society, 15(5), pp.739–768.
- Center for Democratic Transition (CDT) (2024). *Foreign Influences on the Electoral Process in Montenegro 2016–2023*. Podgorica: CDT. Available at: https://en.cdtmn.org/wp-content/uploads/2024/05/CDT-Foreign-Influences-on-the-Electoral-Process-in-Montenegro-2016%E2%80%932023.pdf
- EU Election Observation Mission (2025). *Preliminary Statement - Parliamentary Elections, Kosovo, 9 February 2025*. Pristina: EU EOM, 11 Feb. Available at: https://www.eods.eu/library/EU%20EOM%20Kosovo%202025_Preliminary%20Statement_ENG.pdf
- European Commission, 2020. *Action Plan Against Disinformation*. Brussels.
- European Commission (2023) *Flash Eurobarometer 528: Citizenship and Democracy.* Fieldwork: April–May 2023; Published: 6 December 2023. Luxembourg: Publications Office of the EU.
- European External Action Service – EEAS (2023). *1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. Towards a framework for networked defence. Brussels: EEAS.*
- European External Action Service – EEAS (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence.*
- European External Action Service (2025) *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI).*
- EU StratCom Task Force, 2022. *FIMI Toolbox Overview.*
- Grimmelikhuijsen, S.G. et al., 2013. *The effect of transparency on trust in government: A cross-national comparative experiment. Public Administration Review*, 73(4), pp.575–586.
- Hoffman, F.G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies.
- House of Commons Library (2024). *Romania: recent political developments and 2024 elections* (CBP-10164), 23 December. London: UK Parliament. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-10164/?utm_source=chatgpt.com
- International Republican Institute (2024). Western Balkans Regional Poll February–March 2024. Available at file:///C:/Users/DejanAndonov/Downloads/FINAL-FOR-PUBLICATION-BALKANS-24-RS-01-PT-Megadeck.pdf

- IREX (2023) *Vibrant Information Barometer 2023: Montenegro*. Washington, DC: IREX. Available at:https://www.irex.org/files/vibrant-information-barometer-2023-montenegro.pdf?utm_source=chatgpt.com
- Keohane, R.O. & Nye, J.S., 1998. *Power and Interdependence in the Information Age*. Foreign Affairs, 77(5), pp.81–94.
- Livingstone, S. & Helsper, E.J., 2007. *Gradations in digital inclusion: Children, young people and the digital divide*. New Media & Society, 9(4), pp.671–696.
- Mozilla Foundation (2024). *Election Manipulation in Brazil's 2022 General Elections: The Role of WhatsApp and Telegram on the Attacks Against Electoral Integrity*. 27 February. Available at: https://www.mozillafoundation.org/en/research/library/global-elections-casebook/brazil-case-study/
- NATO, 2020. *Countering Hybrid Threats*. NATO Review.
- OECD, 2017. *Evaluating Development Activities: 12 Lessons from the OECD DAC*. Paris.
- Pamment, J., 2020. *Resilience to Foreign Information Manipulation: The Role of Strategic Communication*. Carnegie Endowment.
- Reuters (2025). '*Does Musk's interview with German AfD leader square with EU laws?*', 9 January. Available at: https://www.reuters.com/world/europe/how-musks-interview-with-german-afd-leader-squares-with-eu-laws-2025-01-09/
- Rid, T., 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
- UNDP, 2021. *Institutional Capacity Assessment Framework*.
- US Army, 2015. *Operational Environment Assessment: PMESII-PT*.
- Wardle, C. & Derakhshan, H., 2017. *Information Disorder: Toward an Interdisciplinary Framework*. Council of Europe.
- Weick, K.E. & Sutcliffe, K.M., 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Wiley.
- Блеер-Симон, К. (2025). *Осврнување на странското мешање и манипулирање со информации во контекст на европските регулативи*. Институт за комуникациски студии. ResPublica, Скопје.
- Bryman, A. (2016) *Social Research Methods*. 5th edn. Oxford: Oxford University Press. Влада на Република Северна Македонија (2021).
- *Национална стратегија за градење отпорност и справување со хибридни закани 2021–2025* (со Акциски план). Скопје.
- Поповска В. (2024). *Информирана одбрана - Вовед за хибридните закани за критичната инфраструктура*. Институт ПРЕСПА – Скопје. Достапно на: http://www.prespa-institute.mk/wp-content/uploads/2024/02/Informirana-odbrana.pdf
- Хаџи-Јанев, М. и Стоилковски, М. (2025). *Странско мешање и манипулирање со информации во Република Северна Македонија: Појдовна анализа*. Скопје: Институт за комуникациски студии. ResPublica. Скопје.

Институт за
комуникациски студии

www.iks.edu.mk

info@iks.edu.mk

British Embassy
Skopje

UK International
Development
Partnership | Progress | Prosperity

Овој производ е подготвен во рамките на проектот „Следење, откривање и разобличување на скриеното странско мешање и манипулирање со информации", финансиран од Владата на Обединето Кралство, со поддршка на британската амбасада во Скопје. Мислењата и ставовите наведени во оваа содржина не ги одразуваат секогаш мислењата и ставовите на британската влада.