СТРАНСКО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Појдовна анализа

СТРАНСКО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ ВО РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Појдовна анализа

DOI: 10.64370/UFCB4462

Институт за комуникациски студии

respublica

Издавач:
Институт за комуникациски студии
ул. „Јуриј Гагарин“ 17-1-1, Скопје
www.iks.edu.mk

За издавачот:
вон. проф. д-р Жанета Трајкоска

Едиција:
ResPublica

Автори:
Вон. проф. д-р Методи Хаџи-Јанев
Д-р Маријан Стоилковски

Уредник:
м-р Дејан Андонов

Лектор:
Ружица Пејовиќ

Графички дизајн:
Игор Делов

Место и година:
Скопје, 2025

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

327.8(497.7)(047.31)
316.776.23(497.7)(047.31)
327.8(4-672ЕУ)(047.31)
316.776.23(4-672ЕУ)(047.31)

ХАЏИ-Јанев, Методи
Странско мешање и манипулирање со информации во Република Северна Македонија [Електронски извор] : појдовна анализа / [автори Методи Хаџи-Јанев, Маријан Стоилковски]. - Скопје : Институт за комуникациски студии, 2025. - (Едиција ResPublica)

Начин на пристапување (URL):
http://respublica.edu.mk/wp-content/uploads/2025/05/stransko-meshanje-i-manipuliranje-so-informacii-vo-rsm.pdf.

- Текст во PDF формат, содржи 73 стр. - Наслов преземен од екранот. - Опис на изворот на ден 02.06.2025. - Фусноти кон текстот. - За авторите: стр. 68. - Библиографија: стр. 69-73

ISBN 978-608-4805-61-8

1. Стоилковски, Маријан [автор]
а) Странски влијанија и дезинформации -- Справување -- Македонија -- Истражувања б) Странски влијанија и дезинформации -- Справување -- Европска Унија -- Истражувања

COBISS.MK-ID 66058757

СОДРЖИНА

	Извршно резиме	6
	Вовед	8
	Методологија	10
1.	**Странско мешање и манипулирање со информации: поим и карактеристики**	12
1.1.	Дефинирање на странското мешање и манипулирање со информации	14
1.2.	Како се манифестира странското мешање и манипулирање со информации	15
2.	**Институционални капацитети и ранливости во Северна Македонија при справувањето со странското мешање и манипулирање со информации**	18
2.1.	Генерален осврт на институционалните капацитети во Северна Македонија за справување со странското мешање и манипулирање со информации	20
2.2.	Законска и регулаторна рамка	21
2.3.	Критички осврт: Институционалните предизвици во Северна Македонија за справување со странското мешање и манипулирање со информации	24
2.3.1.	Преглед на државниот капацитет за одговор на дезинформациски кампањи	29
2.4.	Анализа и критички осврт на улогата на локалната заедница како цел на странското мешање и манипулирање со информации	32
3.	**Улогата на медиумите и граѓанскиот сектор во Северна Македонија и ранливоста од странско мешање и манипулирање со информаци**	34
3.1.	Улогата на медиумите во справувањето со странското мешање и манипулирање со информации	35
3.2.	Улогата на граѓанското општество во справувањето со странското мешање и манипулирање со информации	38

4. Компјутерскиот криминал и социјалните мрежи како алатки за странско мешање и манипулирање со информации 42

4.1. Меѓусебна поврзаност на сајбер-нападите и дезинформациите за манипулација 44

4.2. Компјутерскиот криминал и дезинформациите како ризик на економскиот сектор 47

4.3. Механизми за сајбер-безбедност и заштита од дезинформации 49

4.4. Совети за заштита од сајбер-закани 51

5. Краток осврт на европските добри практики во справувањето со странското мешање и манипулирање со информации 53

5.1. Успешни практики во дел од земјите од ЕУ 55

5.1.1. Јакнење на институционалниот одговор: успешни модели 55

5.1.2. Регулаторна рамка: како правото може да ја заштити демократијата? 56

5.1.3. Јавната свест и медиумската писменост: клучна линија на одбрана 57

5.2. Краток преглед на добрите практики и искуствата на ЕУ и НАТО во справувањето со странското мешање и манипулирање со информации 59

5.2.1. Наменските сили за стратегиска комуникација - Исток на ЕУ (East StratCom Task Force) 59

5.2.2. Центар за извонредност за хибридни закани (Hybrid Center of Excellence): хибридна одбрана преку стратегиска анализа и координација 60

5.2.3. Систем за брзо предупредување на ЕУ(Rapid Alert System): брз одговор на информативните закани 61

Препораки за креирање политики за справување со странското мешање и манипулирање со информации во Северна Македонија 63

Заклучок 66

За авторите 68

Користена литература 69

ИЗВРШНО РЕЗИМЕ

Оваа студија ги истражува механизмите, методите и ефектите на странското мешање и манипулирање со информации (СММИ) (Foreign Information Manipulation and Interference – FIMI) во Република Северна Македонија, со посебен акцент на националната безбедност, медиумскиот колорит и општествената кохезија. Како земја со стратегиска позиција во регионот, членка на НАТО и кандидат за Европската Унија (ЕУ), Северна Македонија се соочува со зголемени информативни закани што доаѓаат од различни државни и недржавни актери. Овие влијанија имаат потенцијал да ги нарушат демократските процеси, да ги ослабат институциите и да поттикнат недоверба кај јавноста.

Студијата покажува дека странското мешање и манипулирање со информации не е изолиран феномен, туку дел од пошироки хибридни стратегии, кои комбинираат дезинформација, геополитички наративи и сајбер-операции за да се обликуваат јавното мислење и политичките одлуки. Во анализата се опфатени повеќе домени, вклучително институционалната подготвеност (со осврт на доброто управување), традиционалните медиуми, дигиталниот простор и социјалните мрежи, локалните заедници и граѓанските организации, при што се идентификувани клучните методи и пристапи што се користат за политичка и идеолошка поларизација.

И покрај постоењето на правни и институционални рамки за справување со странското мешање и манипулирање со информации, националниот капацитет за детекција и спротивставување останува ограничен и неусогласен. Анализата покажува дека е неопходен посеопфатен пристап што ќе вклучува подобра координација меѓу државните институции, граѓанскиот сектор и медиумската заедница. Особено важни се унапредување на доброто управување со државните органи, унапредување на регулаторните механизми за транспарентност во медиумите, зајакнување на аналитичките капацитети за следење на дигиталните закани и градење отпорност кај јавноста преку медиумска писменост.

Оваа студија нуди препораки за унапредување на стратегиите за справување со странското мешање и манипулирање со информации, со фокус на превентивни и реактивни мерки што ќе овозможат заштита на информативниот простор во Северна Македонија. Препораките опфаќаат структурни реформи, подобрување на меѓународната соработка и развој на национални механизми за откривање и

неутрализирање на дезинформациските кампањи. Улогата на државните институции, медиумите и граѓанското општество е клучна во оваа борба, бидејќи само преку заеднички пристап може да се минимизираат последиците од странските информативни влијанија и да се заштитат демократските вредности и безбедносните интереси на земјата.

ВОВЕД

Во современиот глобализиран свет информацијата претставува моќна алатка што може да биде искористена како инструмент за влијание врз општествата, политичките процеси и безбедносните политики. Странското мешање и манипулирање со информации претставува сериозен предизвик за националната безбедност, јавната доверба и демократските институции. СММИ опфаќа широк спектар на активности, вклучително дезинформации, сајбер-напади, медиумска пропаганда и координирани влијателни кампањи, кои имаат цел да ги поткопаат демократските процеси, да предизвикаат поделби во општеството и да ги ослабат државните институции.

Во контекст на Северна Македонија, која е земја-членка на НАТО и кандидат за членство во ЕУ, оваа закана добива особено значење. Како стратегиски позиционирана земја на Балканот, Северна Македонија е изложена на различни форми на странско влијание, кои често вклучуваат манипулација со информации со цел да се наруши јавната доверба во институциите, да се генерира политичка нестабилност или да се попречи евроатлантската интеграција. Надворешните актери, користејќи напредни дигитални алатки, социјални мрежи и традиционални медиуми, сè почесто спроведуваат информативни операции со кои се таргетираат клучни сектори во државата.

Оваа појдовна студија има цел да ги дефинира природата, опсегот и методите на странското мешање и манипулирање со информации во Северна Македонија. Дополнително, ќе се анализираат ранливостите, ризиците и влијанијата врз јавните институции, медиумите и граѓанското општество, со цел да се утврди нивото на изложеност на Северна Македонија кон заканите од СММИ.

Со цел да се добие детална претстава за ранливоста од странско мешање и манипулирање со информации и ефектите што може да се предизвикаат преку ваквото дејствување, анализата ќе се фокусира на неколку главни аспекти. Прво, ќе стане збор за тоа како јавните институции се справуваат со СММИ, а поврзано со тоа и дали постојат структурни или човечки слабости. Во овој дел ќе стане збор за законската и регулаторната рамка, институционалните капацитети и пристапот и способноста да се даде одговор на кампањите за дезинформации. Потоа, анализата ќе се фокусира на медиумите и социјалните мрежи, како и на тоа каква е улогата на локалната заедница (се чини подзаборавен сегмент) како

цел на влијание и во справувањето со овие предизвици. Анализата дава осврт и на фузирањето на сајбер-криминалот и дезинформациите, особено преку социјалните мрежи.

Преку мапирање на постоечките политики и рамки на НАТО и ЕУ, како и механизмите што ги имаат на располагање националните институции, студијата ќе ги идентификува клучните капацитети за спротивставување на странското мешање и манипулирање со информации. Врз основа на оваа анализа, ќе се предложат најдобрите практики и препораки за зајакнување на отпорноста во општествената, медиумската и сајбер-сферата, со крајна цел зајакнување на националната безбедност и демократската стабилност на Северна Македонија.

МЕТОДОЛОГИЈА

Оваа студија се базира на десктоп-анализа како примарен методолошки пристап за истражување на феноменот на странско мешање и манипулирање со информации во Северна Македонија. Овој пристап подразбира собирање, обработка и синтеза на веќе постоечки информации од релевантни извори со цел да се добие сеопфатен увид во природата, методите и влијанието на СММИ врз националната безбедност и општествената стабилност. Овие податоци потоа беа обработени благодарение на професионалното и академско искуство на авторите.

Истражувањето се темели на анализа на официјални документи, извештаи и регулаторни рамки што вклучуваат владини стратегии за справување со хибридни закани, сајбер-безбедност, медиумска писменост и национална безбедност. Дополнително, во анализата се опфатени документи од релевантни безбедносни институции во Северна Македонија, НАТО и ЕУ, како и законски регулативи што се однесуваат на спротивставување на дезинформациите и странското влијание. За подлабоко разбирање на проблемот, студијата вклучува истражувања спроведени од меѓународни тинк-тенкови, истражувачки центри и организации што работат на прашања поврзани со хибридни закани и дезинформации, како што се Центарот за извонредност на НАТО за стратегиски комуникации (NATO StratCom Center of Excellence), Центарот за извонредност за борба против хибридни закани на ЕУ и НАТО (Hybrid Center of Excellence) и Наменските сили за стратегиски комуникации – Исток на ЕУ (East StratCom Task Force), вклучително, и не помалку важно, искуството на авторите во соработката со овие институции на дадената тематика и проблем.

Покрај академските и институционалните извори, анализата опфаќа медиумски публикации и извештаи на невладини организации што се занимаваат со медиумска транспарентност и мониторинг на информативното пространство. Посебен осврт е ставен на улогата што ја имаат медиумите и социјалните платформи во ширењето на дезинформациите.

Методолошки, студијата применува квалитативна анализа на содржината за да ги идентификува клучните наративи, методите и актерите што се вклучени во странското мешање и манипулирање со информации. Овој пристап овозможува систематска категоризација на техниките што се користат во информативните операции, вклучувајќи дезинформација, медиумска манипулација, фабрикување вести, сајбер-напади и геополитички пропагандни стратегии. Покрај тоа, се

користи компаративна анализа за да се спореди македонскиот контекст со слични искуства од други земји во регионот, што овозможува подобро разбирање на моделите и динамиката на заканите од СММИ.

Дополнително, во рамките на истражувањето се анализираат факторите што ја зголемуваат ранливоста на Северна Македонија кон странско мешање и манипулирање со информации, како што се слабостите во медиумската писменост, институционалните капацитети и политичката поларизација. Политичката и нормативната анализа, пак, овозможуваат оценка на постоечките механизми за справување со овие закани, како и нивната ефективност во однос на националните интереси и безбедносните приоритети на земјата.

Иако ова истражување нуди длабинска анализа на странското мешање и манипулирање со информации во Северна Македонија, треба да се земат предвид одредени ограничувања. Недостигот од транспарентни податоци, доверливоста на разузнавачките информации и динамичната природа на дезинформациските кампањи претставуваат предизвик за целосната и објективна проценка на проблемот. И покрај овие ограничувања, оваа студија има цел да даде систематизиран преглед на природата, методите и влијанието на СММИ во земјата, и да изврши мапирање на постоечките политики и механизми за спротивставување на овие закани. Врз основа на овие сознанија, во студијата се предложени препораки за зајакнување на националната отпорност во општествената, медиумската и сајбер-сферата, со крајна цел зајакнување на безбедноста и демократската стабилност на Северна Македонија.

1.

СТРАНСКО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ: ПОИМ И КАРАКТЕРИСТИКИ

Во современиот глобален информативен простор, странското мешање и манипулирање со информации претставува една од најсофистицираните и деструктивни закани за демократските процеси, националната безбедност и општествената кохезија. Овој феномен се засновува на стратегиско и намерно искористување на информациите со цел да се влијае врз одлуките на граѓаните, институциите и владите, најчесто во корист на странски актери.

Странското мешање и манипулирање со информации не е само класична дезинформација. Тоа е комплексен механизам што ги комбинира тактиките на пропаганда, манипулација на медиуми, дестабилизација преку социјални мрежи, економски и политички притисоци, па дури и сајбер-активности. Нивната суштина е во контролираното искривување на информацискиот пејзаж со цел да се постигне долгорочно геополитичко влијание.

1.1. ДЕФИНИРАЊЕ НА СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Наједноставно кажано, странското мешање и манипулирање со информации претставува организирана, намерна и често прикриена активност на државни или недржавни актери насочена кон манипулација на информацискатa околина, заради остварување политичка, воена, економска или социјална предност *(EEA, 2023)*. Клучните карактеристики на СММИ вклучуваат *(Diplomatic Service of EU, 2025):*

- **манипулативен пристап** – преку фабрикувани, манипулирани или селективно презентирани информации за да се создаде лажна слика за реалноста;

- **ваквите активности имаат стратегиска цел** – целта не е само дезинформирање, туку и влијание врз јавноста, институциите или носителите на одлуки и на тој начин да се корумпираат демократските процеси;

- **примена на различни тактики и канали** – употребата на СММИ подразбира комбинирање на методи на класична пропаганда, дигитални манипулации, сајбер-напади, па дури и економски и дипломатски инструменти (на пример, преку повеќеслојна дипломатија или „Multitrack Diplomacy“, односно дипломатија по споредна-втора патека „Track II Diplomacy) *(Diamond L., McDonald J., 1996)*;

- **комплексни се за откривање и следење** – за разлика од конвенционалната дезинформација, СММИ често се спроведува на повеќе нивоа, со комплексни наративи и координирани мрежи на актери, често пати вешто затскриени помеѓу легитимните демократски процеси.

Странското мешање и манипулирање со информации е дизајнирано да дејствува мултидимензионално. Ги напаѓаат институциите, но не директно, туку преку пристап до граѓаните, благодарение на злоупотреба на современите информациски и комуникациски технологии, а во последно време и преку т.н. трансформативни или вознемирувачки технологии што се во подем. Ова им овозможува влијание преку контрола или наметнување контрола врз содржината со која ги (дез)информираат граѓаните, собирање податоци и обработка на тие податоци преку сајбер-напади, манипулација на пребарувачите на интернет и на алгори-

тмите за споделување и пребарување и сл. Според тоа, СММИ не е само закана за индивидуалните корисници на информации, туку и закана за институциите преку создавање информациски хаос, социјални и политички поделби.

1.2. КАКО СЕ МАНИФЕСТИРА СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

СММИ не е ограничено на еден облик на манипулација. Напротив, тоа се манифестира преку различни тактики, кои се приспособуваат на целната држава и конкретниот контекст. Најчестите форми на странско мешање и манипулирање со информации вклучуваат: дезинформации и пропаганда, злоупотреба и манипулација на медиумскиот простор и социјалните мрежи, сајбер-напади, дури и преку посебно наменети алатки за тоа, влијание и манипулација преку економскиот и дипломатскиот сектор за да се засили целокупниот хаос во комбиниран пристап со претходните постапки.

Странското мешање и манипулирање со информации опфаќа напредни методи на класична пропаганда и ширење дезинформации и пропаганда. Тие вклучуваат намерно ширење лажни, искривени или манипулирани информации за да се наруши кредибилитетот на институциите, медиумите или поединците *(Boulianne Sh., Humprecht E, 2023)*. Исто така, СММИ опфаќа и креирање лажни наративи за да се дискредитираат политичките противници или да се зајакне одредена агенда, вообичаено преку користење историски, етнички и религиозни тензии за создавање поделби во општеството *(Miguel R., 2024)*.

Манипулацијата на медиуми и социјални мрежи исто така е техника што е честа во примената на овие практики *(Kelly S. at all, 2017)*. Тоа неретко опфаќа контрола или инфилтрација во локални медиуми, преку различни форми, донации, спонзорства на проекти или, пак, целосно преземање на сопственоста и инсталација на уредувачки одбори склони кон пролиферација на лажни информации и манипулација со информациите наменети за обликување на јавниот дискурс. Манипулацијата со медиумскиот простор вклучува и практика на креирање лажни медиумски платформи што имитираат релевантни извори, но шират пропагандни содржини *(CISA,*

2023). Користењето ботови, тролови и координирани кампањи за масовно распространување манипулативни содржини е дополнителен мултипликатор во манипулациите *(Walker Sh., Simeone M., 2020)*. СММИ често атакува сектори од општеството кои не им даваат приоритет на своите задачи, мисии, ресурси и капацитети за справување со странско влијание. Ова ги зголемува ранливостите низ општеството и бара меѓуопштествен ангажман и координација.

Сајбер-нападите се составен дел на стратегиите за странско мешање и манипулирање со информации. Тоа вклучува:

- **хакирање и изнесување чувствителни податоци,** вклучително и преку напади за откупување (ransomwere) за да се компромитираат политички фигури или институции;

- **спроведување напади преку дистрибуирано попречување услуги (Distributed Denial of Services DDoS)** врз медиумски портали или владини веб-страници за да се намали нивната достапност;

- **лажни дојави или информации** со кои се крева паника за да се парализира или да се тестира, односно да се измести системот и да се создаде кумулативна нетрпеливост кон власта/водството;

- **манипулирање со алгоритмите на социјалните мрежи** за да се промовираат или да се сузбиваат одредени наративи (да се пренасочи сообраќајот, блокира, редуцира или да се забрза, односно пренатрупа).

Иако малку третирано во Северна Македонија, странското мешање и манипулирање со информации често се преточува преку економски и дипломатски канали. Тоа, покрај другото, може да вклучи:

- **искористување стратегиски инвестиции, економска помош, заеми и користење на слободата на пазарот** за стекнување влијание врз медиумите, академските институции или политичките елити, преку трети (вообичаено партнерски) земји;

- **користење на енергетската зависност или трговските врски** за да се наметне политичка агенда;

- **дипломатски притисоци** преку пропагандни медиуми финансирани од странски влади (на пример, „Русија денес“ (Russia Today), „Спутник“ (Sputnik) и други).

Употребата на синхронизирана кампања покажува дека СММИ не се случува спорадично (иако интензитетот може да варира) и не се спроведува случајно. Напротив, зад сите акции лежат стратешки цели кои често имаат за цел (EUEA, 2023):

- **делегитимирање на демократијата и институциите** – поткопување на довербата на граѓаните во нивните влади и создавање перцепција за неефикасност и корупција;

- **политичка поларизација** – поттикнување конфликти помеѓу различни групи во општеството за да се ослаби социјалната кохезија;

- **манипулација на изборни процеси** – влијание врз јавното мислење преку дезинформациски кампањи, особено за време на избори;

- **поткопување на безбедносните сојузи (НАТО, ЕУ)** – создавање перцепција дека западните институции се слаби, поделени или дека не можат да обезбедат стабилност;

- **јакнење на влијанието на авторитарните држави** – промовирање наративи што го претставуваат авторитарниот модел како поефикасен и попожелен од либералната демократија *(EUEA, 2025)*.

Сепак, иако СММИ не е едноставен феномен, неговото влијание може значително да се намали преку стратешки пристап и силна институционална подготвеност.

2.

ИНСТИТУЦИОНАЛНИ КАПАЦИТЕТИ И РАНЛИВОСТИ ВО СЕВЕРНА МАКЕДОНИЈА ПРИ СПРАВУВАЊЕТО СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Манипулирањето со информациите од страна на странски служби директно или преку прокси-актери претставува сериозен предизвик за институциите во Северна Македонија. Во услови на засилена геополитичка конкуренција и дигитализацијата. силен институционален капацитет за справување со СММИ е навистина неопходен. Затоа е потребно разбирање на институционалните ранливости и празнини за да се изготват препораки.

2.1. ГЕНЕРАЛЕН ОСВРТ НА ИНСТИТУЦИОНАЛНИТЕ КАПАЦИТЕТИ ВО СЕВЕРНА МАКЕДОНИЈА ЗА СПРАВУВАЊЕ СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Ова е прва анализа за подготвеноста на институциите во Северна Македонија да се справат со СММИ. Се фокусира на постојната законска и регулаторна рамка, институционалниот капацитет (владините агенции и нивниот пристап – реактивен/проактивен), меѓуинституционалната координација и комуникација и пристапот кон кампањите за дезинформации.

Наодите накратко се дека македонските институции се сè уште во рана фаза во однос на целосно разбирање и ефективно справување со СММИ. Свеста кај политичките претставници за заканата од СММИ е само декларативна. Институционалните претставници ја препознаваат заканата, често како дел од хибридните закани. За жал, во пракса, има многу малку што може да се искористи за реално да се измери дали свеста за заканата е на соодветно ниво (Комисија на ЕУ, 2023). На пример, додека во нивните говори на јавни настани, политичките претставници со право ја препознаваат заканата (МИА, 2022), во пракса може да се види многу малку акција за нејзино спротивставување. На пример, нема податоци за средствата од државниот буџет за градење капацитети за справување со овој предизвик. Наместо тоа, сите активности за обука и зајакнување на капацитетите се одвиваат со финансирање од донатори.

Стратегијата за справување со хибридни закани е единствениот документ кој внимателно се однесува на проблемот на странско мешање и манипулирање со информации (Влада на РСМ, 2021). Документот се наоѓа на веб-страницата на Министерството за одбрана, кое ја предводеше изработката на стратегијата. Додека Владата го задолжи Советот за координација на безбедносно-разузнавачката заедница да го делегира спроведувањето на задачите од Стратегијата и Акциониот план, во пракса овој Совет не е оперативен.

Постоењето на Стратегијата е добар почеток, но треба да се направи повеќе за таа да се операционализира.

2.2. ЗАКОНСКА И РЕГУЛАТОРНА РАМКА

Во Северна Македонија, во законодавството недостигаат специјализирани мерки за странско мешање и манипулирање со информации. Иако одредени одредби што таргетираат теми поврзани со странското мешање и манипулирање со информации постојат во дел од законските решенија, како на пример, Кривичниот законик и Законот за заштита на личните податоци или Законот за изменување и дополнување на Законот за заштита на личните податоци, евидентен е фактот дека овие одредби сами по себе не се доволни за директно справување со СММИ. Отсуството на посебни закони или подзаконски акти што директно го таргетираат странското влијание врз информацискиот простор само потврдува дека законската и регулаторна рамка во земјата за справување со СММИ не е доволно развиена.

Релевантните законски решенија, од каде што би требало да се црпи основата за пристапот во справувањето со странското мешање и манипулирање со информации, ги вклучуваат Законот за кривична постапка, Кривичниот законик, Законот за следење на комуникациите и Законот за електронски комуникации, во кои, меѓу другото, се регулира безбедноста на личните податоци и се дефинираат изрази што имаат битна улога во општењето преку интернет-просторот на македонските граѓани. Дополнително, законски решенија што треба да се земат предвид се и: Законот за медиуми, Законот за аудио и аудиовизуелни медиумски услуги, Законот за спречување на перење пари и финансирање тероризам, Законот за граѓанска одговорност за навреда и клевета, Законот за заштита на децата (кој ги уредува системот и организацијата за заштита на децата) и Законот за правда на детето. Имајќи ја предвид комплексноста на странското мешање и манипулирање со информации, би можело да се каже дека оваа листа на законски решенија не завршува тука. Така на пример, покрај дезинформациите и пропаганда, во доменот на СММИ влегуваат операции за влијание преку сајбер-напади, со цел или да се изменат официјалните информации и да се создаде несигурност и дезинформирање, или да се експлоатира слабата подготвеност на системот за реакција и врз основа на тоа да се прават манипулации и дезинформации. Оттука, ова посочува на потребата од дополнителни законски решенија.

Во текот на изработката на оваа студија, по завршената процедура на Владата пред Собранието на РСМ, е доставен Законот за безбедност на мрежи и информациски системи. Мрежата и информациските системи, а пред сè интернетот,

играат суштинска улога во олеснувањето на малициозното дејствување и примена на странското мешање и манипулирање со информации. Поради таа транснационална природа, значителните нарушувања на овие системи, без разлика дали се намерни или ненамерни и без оглед каде се случуваат, може да влијаат и врз Северна Македонија. Дополнително, со законот се транспонира Директивата (ЕУ) 2016/1148 на Европскиот парламент и на Европскиот совет од 6 јули 2016 година во однос на мерките за висок општ степен на безбедност на мрежа и информациски системи низ Унијата, односно Директивата за заштита на мрежи и информациски системи позната како НИС-директива *(EU Commission, 2022)*.[1] Анализата во овој дел подетално ќе се фокусира на дел од законските решенија.

КРАТОК ОСВРТ НА ОДРЕДБИТЕ ОД КРИВИЧНИОТ ЗАКОНИК (КЗ) НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА

Во Кривичниот законик постојат неколку члена што индиректно може да се поврзат со странското мешање и манипулирање со информации. Така, на пример, во членот 137 од КЗ како казниво дело се смета „поттикнување национална, расна и верска омраза, раздор и нетрпеливост“ и говор што предизвикува омраза и раздор. Сепак, во овој член не се опфаќа влијанието на странски актери или организирани кампањи за дезинформација.

Понатаму, членот 274, кој се однесува на неовластено прислушување и тонско снимање, се однесува на незаконски активности што може да бидат дел од СММИ, но не ја покрива дигиталната дезинформација или странското мешање преку медиумите.

Интересен е и членот 394-г – Терористичка закана, кој се однесува на дела-закани за безбедноста, но не ја опфаќа психолошката манипулација преку информации. Кривичниот законик ќе треба да се развива за да се справи со странското мешање и манипулирање со информации, вклучително и преку:

- јасна дефиниција за „странско манипулирање со информации“;

1 Во оваа директива меѓу другото се инсистира земјите членки да ги подобрат своите способности за сајбер-безбедност, истовремено воведувајќи мерки за справување со ризик и барања за известување на субјекти од повеќе сектори и воспоставување правила за соработка, споделување информации, надзор и спроведување мерки за сајбер-безбедност.

- предвидување санкции за организирани кампањи за дезинформација спонзорирани од странски држави;
- прилагодување на постоењето на дигитални закани и на сајбер просторот.

КРАТОК ОСВРТ НА ЗАКОНОТ ЗА МЕДИУМИ И ЗАКОНОТ ЗА АУДИО И АУДИОВИЗУЕЛНИ МЕДИУМСКИ УСЛУГИ

Законот за медиуми (2013) ги регулира медиумските субјекти и транспарентноста на сопственичтвото. Законот за аудио и аудиовизуелни медиумски услуги (2018, измени 2023) го регулира работењето на радиодифузерите и ги обврзува медиумите на транспарентност во финансирањето. Главни недостатоци на овие законски решенија се:

- немање механизми за спречување странска пропаганда преку националните, регионалните и локалните медиуми;
- немање мерки за медиуми кога свесно шират странско мешање и манипулирање со информации.

КРАТОК ОСВРТ НА ЗАКОНОТ ЗА СПРЕЧУВАЊЕ НА ПЕРЕЊЕ ПАРИ И ФИНАНСИРАЊЕ НА ТЕРОРИЗАМ

Со овој закон, меѓу другото, се регулира и следењето на финансирањето организации и медиуми. Сепак, со оглед на тоа дека не постои јасно усвоена дефиниција за странско мешање и манипулирање со информации преку стратегиски документ за тоа, законот не ја таргетира експлицитно примената на СММИ. Како главни недостатоци на Законот за спречување на перење пари и финансирање на тероризам се издвојуваат следните:

- не постои систем за следење на странското финансирање информативни портали;
- не се регулира финансирањето онлајн-платформи, кои можат да служат за странско мешање и манипулирање со информации.

КРАТОК ОСВРТ НА ЗАКОНОТ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Генерално, со овој закон се регулираат користењето и заштитата на личните податоци. Сепак, со законот не е регулирана злоупотребата на податоци за „таргетирана дезинформација“ или „психолошките операции“, односно операциите за влијание. Оттука, како главни недостатоци се издвојуваат:

- недостиг од механизми за заштита од странски дигитални манипулации (како сценариото од типот на Кембриџ аналитика (Cambridge Analytica) или манипулација од другите т.н. „платформа-компании“)*(Corporate Finance Institute, 2023)*;[2]

- немање јасни процедури за одговор на масовни психолошки операции, односно операции за влијание базирани на злоупотреба на податоци.

2.3. КРИТИЧКИ ОСВРТ: ИНСТИТУЦИОНАЛНИТЕ ПРЕДИЗВИЦИ ВО СЕВЕРНА МАКЕДОНИЈА ЗА СПРАВУВАЊЕ СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Борбата против странското мешање и манипулирање со информации во Северна Македонија е попречена од институционални слабости, ограничени ресурси и неусогласени стратегии. Иако постојат формални механизми и институции што, според законите и другата регулатива, се одговорни за заштита од ваквите закани, нивниот реален капацитет да се спротивстават на координирани дезинформациски кампањи останува загрижувачки низок. Дополнителен проблем е недостатокот на назначувања засновани на заслуги во јавниот сектор.

2 Станува збор за компании што наместо да произведуваат производи или услуги директно, обезбедуваат инфраструктура што им овозможува на трети страни да создаваат вредност. „Платформа-компаниите“ ја трансформираат економијата и начинот на кој луѓето пристапуваат до услуги, често предизвикувајќи ги традиционалните индустрии. Тие се компании што работат како дигитални екосистеми, поврзувајќи различни групи корисници (на пр., купувачи и продавачи, возачи и патници, креатори на содржина и потрошувачи).

Во суштина, македонските институции, како Агенцијата за национална безбедност (АНБ), Министерството за внатрешни работи (МВР), Агенцијата за разузнавање (АР), Воената служба - Секторот за безбедност и разузнавање - (ВСБиР) при Министерството за одбрана (МО) и Националниот центар за одговор на компјутерски инциденти (МКД-ЦИРТ), реагираат на странско мешање и манипулирање со информации на ад хок-основа, без единствена, централизирана стратегија што би овозможила ефикасен, координиран одговор.

Агенцијата за национална безбедност (АНБ), која има мандат за контраразузнавачки операции, има потреба од развиен специјализиран тим што се занимава со дигитални дезинформации и хибридни закани. Таа најчесто се потпира на традиционалните методи на разузнавање. Овие методи во услови на современа информациска војна, во која има и операции на влијание, злоупотреба на сајбер-просторот и т.н. напади под „прагот на класичната употреба на сила“ преку технологии, веќе не се доволни. Поголем предизвик претставува тоа што АНБ нема јасни овластувања за справување со онлајн-манипулации на јавното мислење, особено кога тие не се директен резултат на странски разузнавачки служби, туку на парадржавни или „сива“ мрежа на актери што користат локални медиуми и социјални мрежи како алатки за влијание. Без јавен документ за градење на капацитетите на АНБ во оваа насока, не е јасно дали ситуацијата се решава.

Секторот за компјутерски криминал на Министерството за внатрешни работи (МВР) главно се занимава со класични сајбер-престапи како финансиски измами и хакирање. За структурирана анализа на мрежите за дезинформации, Секторот би имал корист од повеќе професионално обучени вработени, експерти за дигитална форензика, софистицирани алатки за следење дигитални кампањи, како и подлабока соработка со глобалните технолошки компании како Мета (Meta), Гугл (Google) и Икс (X).

Агенцијата за разузнавање (АР) на сличен начин има потреба од човечки и технички капацитети. Иако има напори за градење на капацитетите преку билатерална или мултилатерална соработка, овие напори не се планирани или финансирани од самата агенција, туку се обезбедени преку донаторски проекти.

Воената служба – Секторот за безбедност и разузнавање при Министерството за одбрана, се соочува со сличните предизвици. Министерството и Армијата на Република Северна Македонија (АРСМ) немаат развиено доктрина за намалување на ризикот за припадниците на армијата и цивилниот персонал во вооружените сили и министерството и нивните фамилии во земјата, така и за војниците

и цивилниот персонал што се распоредени на извршување должности во мисиите предводени од НАТО, ЕУ или ОН. Иако постои воен авторитет за сајбер-одбрана, тој главно е фокусиран на заштита на критичната инфраструктура, а не на анализа на хибридни закани што вклучуваат информациска војна и операции за влијание. Ова е особено загрижувачко ако се има предвид дека современите воени доктрини на Русија, Кина, но и терористички групи со глобална агенда, силно се потпираат на информациски операции како дел од нивната стратегија за проекција на моќ. Иако во рамките на Армијата психолошките операции се третирани до одредена мера, целиот пристап е на базично рамниште со фокус на експедициските операции на армијата, а не во контекст на уставната должност за одбрана на територијалниот интегритет и суверенитет. Кога на тоа ќе се додаде и законското ограничување за дејствување на Армијата на територијата на државата, тогаш е јасно дека овој капацитет е несоодветен за заканата од СММИ.

Со оглед на тоа дека во рамките на ЕУ дезинформациите од 2023 година се составен дел на сајбер-заканите (CERT–EU, 2024). Националниот центар за одговор на компјутерски инциденти (МКД-ЦИРТ) во рамките на Агенцијата за електронски комуникации треба во континуитет да ги зајакнува човечките и останатите капацитети за извршување на основната функција – справување со сајбер-инциденти и за следење на трендовите на ЕУ и НАТО во овој контекст. Имено, ЕУ на дезинформациите гледа како составен дел од сајбер-безбедноста, а НАТО од 2015 година смета дека сајбер-просторот е посебен домен на војување и оттука при планирањето на сајбер-безбедноста треба да се планираат и одговори и операции за справување со операциите за влијание *(Hubervic A., Prudent Y., STO)*. Дополнително, сајбер-безбедноста, а со тоа и заканите од дезинформациите и манипулација преку влијание се дел од националната безбедност.[3]

Друг критичен аспект во овој контекст е тоа што Агенцијата за аудио и аудиовизуелни медиумски услуги (АВМУ) има ингеренции за социјалните платформи само ако се регистрирани во земјата, а такви нема *(Законот за аудио и аудиовизуелни медиумски услуги, 2014)*. Странските и домашните центри за дезинформации можат да ја користат оваа правна празнина за да создадат и да одржуваат портали што немаат јасно дефинирана сопственост и кои можат да исчезнат и за само неколку часа повторно да се појават под различно име.

3 На пример, во Стратегијата за сајбер-одбрана, која е со одминат рок, се препознава дека членот 5 може да биде правна основа за водење физички воени операции и употреба на сила како одговор на сајбер-напади.

Странското влијание со дезинформации, како и секаде, има посебна тежина врз изборните процеси. Оттука, Државната изборна комисија (ДИК), која е одговорна за транспарентноста на изборниот процес, треба да ги подобри капацитетите за мониторинг на дигиталното мешање во изборите. Во спротивно, во најлош случај, странските актери би можеле неказнето да шират лажни информации за изборни процеси, да користат ботовски мрежи за дискредитација на одредени кандидати, па дури и да влијаат врз изборните резултати преку кампањи наменети за одвраќање на гласачите. Во овој контекст вреди да се спомене и тоа дека онлајн-портали регистрирани во странство можат да добиваат средства за политичките кампањи во земјата.

Институционалните слабости не се одраз само на предизвиците што доаѓаат од недостигот од технички или човечки ресурси. Суштинскиот проблем лежи во недостигот од координација и политичка волја за сеопфатен пристап кон решавање на ова прашање. Северна Македонија нема посебен национален центар за борба против дезинформациите. Постоечките органи што треба да го покријат овој дел често се без јасен механизам за размена на податоци и разузнавачки информации или се нефункционални. Така, на пример, Советот за координација на безбедносно-разузнавачката заедница, кој е задолжен за борба против хибридни закани, е нефункционален и не овозможува размена на информации на институционално ниво. Дополнително, не постои дигитална поврзаност помеѓу институциите, па во случај на проблем, често заради организациската поставеност и различните позиции на потчинетост (што е добро заради децентрализација и избегнување на акумулирање моќ), не е јасно која институција потфрлува или има надлежност за даден проблем. Ова создава опасен вакуум, кој странските актери можат да го користат за непречено ширење наративи и други форми на влијание што ги поткопуваат демократските процеси и националната безбедност.

Уште една слабост е отсуството на повеќе и позачестени институционални иницијативи за зголемување на јавната свест за странското мешање и манипулирање со информации и на информацискатa и медиумската писменост на населението. Институцијата што има законски мандат да ја промовира медиумската писменост преку соработка со граѓански организации, образовни институции, медиуми и институции е ААВМУ. Во 2017 година таа ја формираше Мрежата за медиумска писменост, сега со преку 80 члена (министерства, државни институции, образовни институции, граѓански здруженија и организации и медиуми), и еднаш годишно спроведува кампања од јавен интерес во соработка со медиумите, посветена на медиумската писменост и безбедноста при користењето на

интернетот и социјалните медиуми[4]. Сепак, голем дел од македонските граѓани немаат знаења, вештини и алатки за препознавање манипулативни наративи, што ги прави ранливи на влијание од различни пропагандни извори. Оваа состојба е влошена од фактот што дел од домашните политички елити користат дезинформации како алатка за политичка пресметка, придонесувајќи, свесно или несвесно, во засилување на странското мешање и манипулирање со информации. Блискоста на јазиците (српско-хрватскиот и албанскиот) е дополнителен проблем, кој во ера на отворени општества и слободен пазар исто така бара внимателен пристап.[5]

Соочени со оваа реалност, институциите во Северна Македонија мора да преземат одлучни чекори за подобрување на капацитетите и воспоставување стратегија за национална отпорност на странско мешање и манипулирање со информации. Ова подразбира:

- сеопфатен пристап кон борбата против дезинформациите и задолжување орган што ќе ги координира сите државни актери во оваа смисла;
- јакнење на капацитетите на АНБ, АР, МВР, МО и АРСМ за следење и неутрализирање на СММИ;
- зголемена соработка со НАТО, ЕУ и технолошките компании за справување со сајбер-дезинформациите;
- унапредување на медиумската и информациската писменост во образовниот систем како долгорочна стратегија за градење отпорност.

Доколку овие мерки не се преземат на време, државата ќе остане ранлива на странски информативни манипулации, што долгорочно може да ја поткопа не само демократијата, туку и националната безбедност.

4 Види повеќе на: https://mediumskapismenost.mk/

5 Странските актери или локалните дезинформатори што се окупирани, поткупени или, пак, купени, можат брзо да адаптираат наративи од еден јазик на друг, или, пак, да го пласираат само на српско-хрватски или албански јазик. На тој начин, од еден центар (Белград, Тирана и сл.) може да влијаат врз целиот регион. Тоа овозможува координирано ширење лажни информации во различни етнички заедници, особено ако се знае и фактот дека голем број локални медиуми заради оскудните капацитети често преземаат информации од овие центри. Оваа јазична сличност може да биде искористена и за создавање лажни преводи, дезинформациски кампањи со манипулирани цитати или фабрикувани вести што звучат автентично за повеќе групи, но и да бидат разбрани од поголема публика. Ова е особено опасно во чувствителни контексти како политички кризи, избори или меѓуетнички тензии, каде што манипулираните пораки можат да поттикнат недоверба, поделби и дестабилизација.

2.3.1. ПРЕГЛЕД НА ДРЖАВНИОТ КАПАЦИТЕТ ЗА ОДГОВОР НА ДЕЗИНФОРМАЦИСКИ КАМПАЊИ

Државниот капацитет за одговор на дезинформациски кампањи, како најзначаен дел за справување со странското мешање и манипулирање со информации, накратко би можело да се сумира дека е ограничен за следење и анализа. Дополнително, во Северна Македонија има слаб институционален капацитет за давање сеопфатен темелен и навремен одговор преку креирање соодветен наратив. Целата оваа институционална слабост е проследена со недоверба во институциите. Во делот што следува, преку анализата на овие три параметри - капацитетот за следење и анализа на дезинформациите, стратегиското комуницирање и формирање контранаратив и граѓанската доверба во институциите, ќе се даде осврт на државниот капацитет за одговор на дезинформациски кампањи.

КРАТОК ОСВРТ НА ДРЖАВНИОТ КАПАЦИТЕТ ЗА СЛЕДЕЊЕ И АНАЛИЗА НА ДЕЗИНФОРМАЦИИТЕ

Во современиот информативен простор дезинформациите се шират со невидена брзина. Алгоритмите на социјалните мрежи ја поттикнуваат поларизацијата, а странските актери користат локални медиуми, тролови и ботовски мрежи за да ги засилат своите наративи.

Државните институции немаат доволно развиени механизми за мониторинг на странското мешање и манипулирање со информации, заради што често се потпираат на анализи од невладиниот сектор и меѓународни партнери. Иако овие анализи се добри и пожелни, самите по себе не се доволни и немаат државнички предзнак.

Иако како земја членка на НАТО, Северна Македонија добива голема помош од Центарот за извонредност за стратегиски комуникации (NATO StratCom CoE) и, како земја аспирант за ЕУ, од иницијативата на ЕУ за борба против дезинформации EUvsDisinfo, овие механизми имаат само консултативна улога. Дури и кога надворешните партнери ќе алармираат за дезинформациски напади насочени кон државата, институциите треба да имаат соодветен механизам за реакција. Оттука, потребен е институционален пристап со кој би се стеснил просторот за маневар на малициозните, често прокси-државни и недржавни актери.

ОСВРТ НА НАЦИОНАЛНИТЕ КАПАЦИТЕТИ ЗА КРЕИРАЊЕ НАРАТИВ

Во Северна Македонија е евидентно бавното и неефективно спротивставување на дезинформациските кампањи, што остава простор за нивно засилување. Покрај немањето капацитети за мониторинг, македонските институции немаат јасен и убедлив контранаратив што би им парирал на дезинформациите и честопати ниту одговараат брзо, ниту ги негираат или објаснуваат дезинформациите. Како резултат на тоа, невистините во јавниот простор се шират со голема брзина. На пример, кога Северна Македонија се најде под удар на дезинформациски кампањи за членството во НАТО, кои промовираа наративи за „украдени национални ресурси“ и „воено вклучување на земјата во конфликти“, институциите не успеаја навремено да комуницираат со јавноста. Наместо проактивен пристап со јасни пораки и докази, реакцијата на државата беше ограничена на општи изјави, без стратегиски осмислена комуникација. Таков пример имаше и при сајбер-нападот на Фондот за здравствено осигурување, за што постои сериозна загриженост за кражба на огромен број податоци на граѓаните.

Дополнителен проблем е што македонските владини претставници често користат комплициран бирократски јазик. Овој јазик не е приспособен и со тоа е неефективен во дигиталната ера. Дезинформациите, од друга страна, се формулирани на едноставен и емотивен начин, што ги прави подостапни и влијателни за широката јавност. Тие артикулираат емоции, будат емпатија, атакуваат вредности, подриваат доверба, често се стилски добро обликувани со хиперболи, несоодветни компарации, занемаруваат клучни моменти што може да му дадат поинаков тек на нивниот аргумент-теза и нагласуваат проблематични аспекти што им служат на нивните цели. Дури и кога нема директна врска, имплицираат на етнички прашања, политички разочарувања и историски проблематични теми, преку себепроклами-рана легитимност или изваден од контекст и нецелосно претставени тези на етаблирани научници и експерти.

Друг клучен аспект е немањето единица, оддел или тело за брз и координиран одговор на дезинформациски напади. Во многу држави ваквите тела се дел од премиерските канцеларии или министерствата за надворешни работи. Оттука, заради комплексноста и диверзитетот на областите и темите преку кои се шират дезинформациите, многу често давањето несоодветни или нецелосни изјави од официјалните владини претставници може да е само по себе можност за манипулација и дезинформации. Во практиката новинарите често немаат капацитет соодветно да известуваат бидејќи немаат тематска и стручна подготвеност, па пренесуваат информација што е делумна, често лошо формулирана и/или не е

докрај точна. Како последица на тоа, се воспоставува информациски хаос, што дополнително го еродира капацитетот на државните органи да се справат со дезинформациите, а со тоа и јавната доверба.

ЈАВНАТА ДОВЕРБА ВО ИНСТИТУЦИИТЕ КАКО ЕЛЕМЕНТ ЗА СПРАВУВАЊЕ СО ДЕЗИНФОРМАЦИИТЕ

Во јавноста често преовладува мислењето дека самите институции се извор на манипулации, што дополнително ја комплицира борбата против странското мешање и манипулирање со информации. Дел од граѓаните ги гледаат институциите како дел од проблемот, а не како решение *(Јакимова Ј., 2022)*. Ваквата недоверба генерално произлегува од неколку фактори, како политичката инструментализација на информациите, корупцијата и злоупотребата на политичката моќ, лошо организираните и неуспешни комуникациски кампањи.[6] Во таа смисла, јавноста често сведочи на политички мотивирани интерпретации на фактите, што ја намалува кредибилноста на официјалните извори. Многу граѓани веруваат дека институциите не работат во нивен интерес, што ги прави подложни на дезинформации. Тоа често во практиката се преведува како „Западот ја контролира земјата“ или „Северна Македонија е марионетска држава“. Конечно, недостатокот на транспарентноста е сериозен хендикеп што е препознаен во низа извештаи на независни тела, но и на ЕУ *(Европска комисија, 2021)*. Институциите често одговараат со негирање или игнорирање на контроверзните теми, што само ја продлабочува кризата на доверба.

6 На пример, стручно мислење е дека по смената на власта како резултат на скандалот со прислушувањето во 2017 година новите (сега веќе опозициски) лидери како да ја прифатија истата стратегија или консултантска услуга за односи со јавноста. Поедноставено, не се смени ништо во овој дел. Во неколку наврати извештајот на ЕУ за Северна Македонија од 2023 година го нотира сето ова.

2.4. АНАЛИЗА И КРИТИЧКИ ОСВРТ НА УЛОГАТА НА ЛОКАЛНАТА ЗАЕДНИЦА КАКО ЦЕЛ НА СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Локалните заедници во Северна Македонија играат клучна улога во сложената мрежа на дезинформации и странско влијание. Тие се и цел на манипулација и потенцијален фактор на отпор. Дезинформациските кампањи ги таргетираат локалните заедници преку национални и локални медиуми, социјални платформи и мрежи на неформални актери, со цел да предизвикаат недоверба, поделби и дестабилизација.

Локалните заедници се идеални цели за операции за влијание од едноставна причина што целта на влијанието и информациските операции е да се искористат празнините што постојат во ефективното управување со локалните институции во демократските општества. Оттука, децентрализацијата на управувањето и институциите отвора голем број ранливости за безбедноста на државата. Имено, слабостите во управувањето со локалните институции се искористуваат со операции за манипулација. Најчесто локалните заедници се на првата линија на информациската војна, бидејќи странските актери ги користат постојните етнички, политички и економски разлики, но и лукративните амбиции на локалните и политичките елити за да предизвикаат нестабилност.

Фактот дека македонското општество е мултиетничко, во контекст на целиот сплет на околности (локални динамики и геостратегиски амбиции), локалната заедница во државата е неминовно ранлива на дезинформациски наративи што го поттикнуваат меѓуетничкиот раздор. Проруски канали често шират дезинформации дека „Западот ги уништува традиционалните вредности“ или дека „НАТО ја потиснува македонската култура“ *(Вистиномер, 2023)*. Овие наративи се надоврзуваат со интегративните процеси на ЕУ *(Stanicek B. Caprile A., 2023)* и дефокусот на САД од регионот *(CSIS, 2021)* и, како резултат на тоа, со „несреќното чувство“ за непожелност. Засилување на целиот тој колаж се историските „проблематични сентиментални вистини“ што туркаат дел од македонското етничко граѓанство кон т.н. десни политички наративи и барање за чиста етничка национална припадност. Албанските заедници, истовремено, се таргетирани со приказни дека „македонската држава не ги штити нивните права“, што ги зајакнува

сепаратистичките чувства *(Koldomasov A., Pylypenko A., 2024)*. Кога на сето ова ќе се додаде политизацијата на овие прашања за добивање политички поени и за да се покријат корупцијата, лошото управување, нетранспарентноста и немањето отчетност, јазот на довербата во институциите само се засилува и се проширува просторот за странско влијание. Суперзасилување на целата оваа комплексна ситуација се наративи што го разгоруваат прашањето за македонскиот идентитет, користејќи локални медиуми и влијателни личности за да поттикнат недоверба кон официјалните институции *(Vatsov D. at all, 2023)*.

Локалните заедници, особено во помалите градови, се ранливи на лажни информации поврзани со економијата. Дезинформациските наративи често шират паника, тврдејќи дека „ЕУ не ѝ носи ништо добро на земјата“ или дека „кинеските и руските инвестиции се посигурни и попрофитабилни“. Кога се најавуваат големи проекти (на пример, инфраструктурни инвестиции), кампањите за дезинформации може да ги претстават како „перење пари“ или „продажба на националните интереси“. Сето ова со претходно опишаните слабости и ранливости ја поткопува довербата во легитимните економски реформи *(„По патот на Македонија“, 11.01.2025)*.

Инструментализацијата на религијата и на традиционалните вредности е дополнителен комплексен феномен што во екот на демократското општество и слободата на вероисповедта се експлоатира за странско мешање и манипулирање со информации. Верските институции во локалните заедници често се користат како канали за ширење одредени дезинформации, како за целите на одредени државни актери, така и за одредени недржавни актери. Ова особено се забележува во наративите против ЛГБТ+ заедницата, мигрантите или промените во образовниот систем, кои се претставуваат како „западно влијание што ги разорува традиционалните вредности“.

3.

УЛОГАТА НА МЕДИУМИТЕ И ГРАѓАНСКИОТ СЕКТОР ВО СЕВЕРНА МАКЕДОНИЈА И РАНЛИВОСТА ОД СТРАНСКО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

3.1. УЛОГАТА НА МЕДИУМИТЕ ВО СПРАВУВАЊЕТО СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Медиумскиот пејзаж во Северна Македонија е комплексен и исполнет со политички, економски и надворешни влијанија, што го прави исклучително подложен на странско мешање и манипулирање со информации. Доминиран од политички контролирани медиуми, зависни приватни телевизии, онлајн-платформи со слаби стандарди за известување и распространети дезинформации на социјалните мрежи, медиумскиот простор ја зголемува ранливоста на државата.

Медиумите можат да бидат предмет на сериозен политички притисок, што резултира со притисок што ја поткопува нивната примарна функција како чувар на општеството. Истовремено, да не бидат независен сервис на граѓаните што ќе обезбеди платформа за различни гласови и мислења, овозможувајќи плурализам и активна граѓанска партиципација *(BIRN Macedonia, 2023)*.

Националната радиотелевизија (Македонската радио-телевизија - МРТ), како главен јавен радиодифузен сервис, има потенцијал да биде важен столб на професионално и непристрасно новинарство. Сепак, политичкиот притисок и недоволното финансирање може да ја компромитираат нејзината улога. Иако номинално независна, МРТ често се наоѓа под влијание на партиските елити *(Tuneva M., 2023)*. Немањето соодветни ресурси е дополнителен предизвик во работата на јавниот сервис што ја ограничува продукцијата на квалитетна новинарска содржина и истражувачко новинарство во борбата против дезинформациите *(Association of Journalists of Macedonia, 2023)*.

Доминацијата на политичко-економските интереси е застапена и помеѓу приватните медиуми. Различни студии покажуваат дека медиумите што се во сопственост на бизнис-групациите често одржуваат блиски односи со политичките елити. Ова резултира со медиумска пристрасност, автоцензура и ограничен простор за критичко новинарство *(Tuneva M., 2023)*. Состојбата тешко се менува и медиумите не го стимулираат истражувачкото и тематски ориентирано новинарство, што ќе ги зајакне професионалноста и пристапот, меѓу другото, и кон проблемот со странското мешање и манипулирање со информации.

Ваквата поставеност е совршена за стратегиите на антидемократските малициозни центри и прокси-актери на предизвикувачите на евроатлантската агенда. Фрагментираноста во регулативите и примената на законските решенија и испреплетеноста на бизнис- и политичките интереси остава простор за странско влијание преку финансиски поттикнати наративи. Некои анализи укажуваат дека е голема веројатноста одредени медиуми да примаат финансиска поддршка од странски центри на моќ (Русија, Србија, Бугарија, Турција, Кина), што се одразува преку агресивна промоција на нивните интереси *(Association of Journalists of Macedonia, 2023; Фајфер Х., 2024)*.

Сепак, главен канал и извор за дезинформации претставуваат онлајн-медиумите. Дигиталниот простор и можноста за дејство од далечина, во услови на крајно проблематична автентичност и можност за манипулација на дигиталниот идентитет и извор, е можеби најранливиот сегмент во медиумската структура. Сопствениците и начините на финансирање на онлајн-порталите често се непознати, што остава простор за лесна манипулација. Токму овие портали се најголемиот извор на сензационалистички вести, непотврдени информации и директни дезинформации, без јасни одговорности за објавената содржина. Но еднозначната систематизација и категоризација на овие медиуми како проблем или нивното сузбивање во услови на отворени пазари и различни интерпретации на слободата на говорот се крајно отежнати. Тоа може да води кон грешка и медиуми што не се дел од овие мрежи да се идентификуваат како да се. Ваквата состојба ја зголемува можноста за камуфлажа бидејќи нивната адаптација, меѓу другото, е и во насока на потхранување на информацискиот хаос. Во такви услови, овие портали лесно се претвораат во ботови и фабрики за лажни информации, а преку нив се организираат кампањи на социјалните мрежи (Фејсбук, Инстаграм, Тикток, Икс), со што значително влијаат врз јавното мислење преку автоматизирани профили и координирани активности.

Ова нè води до уште еден клучен аспект — улогата на социјалните медиуми во ширењето на СММИ. Социјалните медиуми се најголемата зона на неконтролирано влијание и функционираат како катализатор за дезинформациски кампањи, бидејќи ги заобиколуваат традиционалните медиумски стандарди и лесно таргетираат специфични групи на население. На Фејсбук, на пример, постојат групи што шират конспиративни теории успешно приспособени на дадени социјални или геополитички моменти и се адаптирани на домашните проблеми или неукоста на политичките елити за справување со дезинформациите. Така, на пример, во времето на ковид-19, антиваксерските наративи беа доведувани во политички контекст со величење алтернативни партнерства, а во времето на зачленувањето

во НАТО, шириа анти-НАТО и анти-ЕУ пропаганда. Телеграм групите, пак, функционираат како затворени заедници во кои дезинформациските наративи се засилуваат без никаква контрола, создавајќи т.н. ефект на екоќелии на истомисленици, во кои секое спротивно мислење однапред се отфрла, идеално за радикализација што може да има екстремистички погледи и да упатува или да повикува на насилство. Сето ова, во амалгамот од политизацијата на секој сегмент на општеството, има сериозна почва во ниската медиумска и информациска писменост. Голем дел од населението не прави разлика помеѓу кредибилни извори и дезинформациски кампањи, што ја олеснува манипулацијата *(Институт за комуникациски студии, 2024)*.

Како резултат на ваквиот медиумски пејзаж, Северна Македонија е високо ранлива на странско влијание и дезинформациски кампањи. Ова се одразува во неколку клучни аспекти:

1. поларизација на општеството во кое политички контролирани медиуми и дезинформации на социјалните мрежи го засилуваат општествениот раздор;

2. недоверба во институциите, при што граѓаните постојано се изложени на лажни информации и манипулативни наративи, а нивната доверба во медиумите и официјалните извори опаѓа;

3. во услови на ниска свест и капацитет за справување со оваа форма на влијание, политичките елити во земјата во изминатите десетина години не успеаја да изградат систематски пристап (нема стратегија ниту впечатлива политика) за справување со дезинформациите, што ја остава државата ранлива; и

4. непречена промоција на странски политички и економски интереси без посебен државно уреден филтер што ќе биде одраз на јасниот курс на евроатлантската агенда. На тој начин, одредени медиуми може да промовираат агенди на трети земји и директно да ги поткопуваат македонската надворешна политика и интегративните процеси во ЕУ и НАТО.

3.2. УЛОГАТА НА ГРАЃАНСКОТО ОПШТЕСТВО ВО СПРАВУВАЊЕТО СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Граѓанското општество во Северна Македонија игра клучна улога во борбата против странското мешање и манипулирање со информации. Меѓутоа, заради можеби архаичниот пристап во управувањето (специфичен за поранешниот систем на доминантна улога на државата во граѓанското општество), граѓанскиот сектор нема институционална поддршка со која би се искористил потенцијалот за справување со СММИ. Невладините организации, медиумските здруженија и индивидуалните експерти се меѓу ретките актери што системски анализираат, разобличуваат и едуцираат за дезинформациите. Сепак, нивното влијание е ограничено поради неколку клучни предизвици: ниското ниво на медиумска писменост, ограничените ресурси, недоволната државна поддршка и, како што е претходно објаснето, недовербата во институциите.

Ниското ниво на медиумска и информациска писменост ја прави јавноста подложна на манипулации, особено во дигиталниот простор *(Институт за комуникациски студии, 2023),* што пак ја продлабочува ранливоста на странското мешање и манипулирање со информации. Во време на конвергенција на дигиталниот и физичкиот свет, образованието засега не успева да фати чекор во подготовката и приспособувањето на населението на дигиталниот простор (дури ни на младите, кои се најголеми корисници на електронските информации). Иако постојат иницијативи за медиумска писменост, формалното образование треба да воведе поинтензивна едукација за проверка на факти, дигитална писменост и препознавање пропаганда. Навиките и претпоставките за консумирање на информациите од традиционалните медиуми, кои имале изграден професионален авторитет од минатото, пред сè во поглед на легитимноста и веродостојноста на содржината и се земале „здраво за готово“, сега се применуваат и при консумирањето информации од дигиталните медиуми. Дигиталната џунгла, во која секој може да креира содржина и да наметне авторитет, во услови на ниско ниво на медиумска и информациска писменост, ги прави граѓаните лесен плен на економските, но и на политичките предатори. Како резултат на таа неподготвеност, сè уште голем дел од населението не поседува вештини за разликување на кредибилните извори од дезинформациите, што дозволува брза циркулација на лажни наративи.

Политичката пристрасност е дополнителен фактор што ги засилува опасноста и можноста за дезинформации. Македонската јавност е силно политички поларизирана, што значи дека луѓето често ги прифаќаат информациите што ги потврдуваат нивните предрасуди, без да ги проверуваат изворите. Паралелно со претходните две слабости, населението е жедно за сензационализам и толерантно на ниски новинарски стандарди ако содржината одговара на политичката припадност или интерес. Многу медиуми ги поттикнуваат дезинформациите со сензационалистички наслови и неконтролирано преземање содржини од социјалните мрежи. Блискоста на јазикот и консумирањето информации од извори и медиуми од државите во регионот на Западен Балкан може да биде дополнителен катализатор за дезинформации што се шират регионално *(Reporters Without Borders, 2024; Blue Europe, 2024)*. Сето ова влијае, свесно или несвесно, граѓаните да учествуваат во ширењето на дезинформациите, без да имаат капацитет да ги идентификуваат намерите зад тие наративи.

Во отсуство на силен институционален одговор на странското мешање и манипулирање со информации, граѓанскиот сектор ја презема главната улога во анализата и разобличувањето на дезинформациите. Невладините организации и независните истражувачи имаат клучна улога во:

а) мониторингот и анализата на дезинформациите;

б) едукацијата претежно за медиумската писменост, иако има сегментен пристап на целосно вклопување и на информацискатa писменост; и

в) јавниот притисок и застапувањето политики.

Неколку граѓански организации во Северна Македонија активно работат на зголемување на отпорноста на населението на дезинформации, особено во дигиталниот простор, подигнувајќи ја свеста за дезинформациите, што придонесува и за справување со странското мешање и манипулирање со информации. Тие иако го надополнуваат недостигот во државните програми за медиумска и информациска писменост, имаат ограничено влијание бидејќи не се дел од формалниот образовен систем. Како резултат на УСАИД-проектот за медиумска писменост „Младите размислуваат“, кој во изминатите четири години беше спроведуван од Македонскиот институт за медиуми, Институтот за комуникациски студии и Младинскиот образовен форум, а во соработка со Министерството за образование и наука (МОН) и Бирото за развој на образованието (БРО), медиумската писменост беше вклучена во основното образование, во предметите по мајчин јазик во сите години. Беа обучени повеќе од 8.000 наставници и беше изработена

Рамка за медиумска писменост за основно образование со цел да се обезбедат основни вештини и структурирани насоки за интегрирање на медиумската писменост во наставниот процес. Во основното образование се изучуваат и други предмети што опфаќаат сегменти од медиумската писменост и вештини за дигиталната писменост. Во средното образование, пак, наставните програми ги опфаќаат медиумите како содржина, но без посебен акцент на медиумската писменост. Само некои од прашањата поврзани со медиумската писменост се обработуваат во различни предмети. Во високото образование, како резултат на УСАИД-проектот во изминатите три години, изборни предмети за медиумска писменост се воведоа на 8 факултети, меѓу кои оние што регрутираат наставници за основно и средно образование. Проектот придонесе и во неформалното образование преку отворање клубови за медиумска писменост во 30 основни и 10 средни училишта и организирање медиумски и новинарски обуки и работилници за средношколци и останати млади луѓе, во кои беа вклучени повеќе од 2.000 млади луѓе. Сепак, според националниот извештај од Мониторингот на медиумскиот плурализам во дигиталната доба за 2023 година *(Мицевски И., Трпевска С., 2024)*, што се спроведува во земји членки и кандидатки на ЕУ, степенот до кој медиумската писменост е вградена во формалното образование е незадоволителен, а истиот заклучок може да се донесе и за неформалното образование.

Јавниот притисок и застапувањето политики се следниот механизам преку кој НВО се обидуваат да го третираат проблемот со странското мешање и манипулирање со информации. Во овие напори се алудира за транспарентност во медиумите, подобрување на законската рамка, се одржуваат јавни дебати во соработка со медиумите и сл.

Сепак, еден од најголемите предизвици на работата на граѓанските организации е одржливоста на напорите. Нивната работа често зависи од одреден проектен циклус и не може да биде одржлива на долг рок. Манипулациите што го следеа овој сектор базиран на блиските односи со властите остваат простор за сомнеж околу независноста во нивната работа *(Клинчарски П., Гаџовска Спасовска З., 2024)*.

Следен проблем и недостаток е немањето заштита од политички напади и дискредитација. Одредени НВО што разобличуваат дезинформации се цел на политички и медиумски напади, при што се обвинувани како странски агенти, што заедно со дел од обелоденетите скандали за корупција и во овој сектор *(Клинчарски П., Гаџовска Спасовска З., 2024)*, ја намалува нивната кредибилност во очите на јавноста.

Следен недостаток и ограничување е и фактот дека отсуствува соодветен капацитет или ангажман за идентификација на мрежи на дезинформација и влијание со примена на одредени техники, како ОСИНТ (OSINT) – анализа на информации од отворен карактер (извори), дигитална форензика и анализа на алгоритми. Добрите практики укажуваат дека граѓанскиот сектор може да има значајна улога во мапирањето на координираните мрежи на ботови и манипулативни медиуми што ја таргетираат македонската јавност. Тоа укажува на потребата од интердисциплинарен пристап, во кој би биле вклучени безбедносни и сајбер-експерти што имаат не само технички, туку и безбедносно-разузнавачки, но и лингвистички вештини (на пример, идентификација на манипулации преку т.н. феномен „податочни празнини“ (data voids) или минимални, нискоквалитетни или манипулативни информации од пребарувачите кога има голема побарувачка за информации за одредена тема, но малку веродостојни извори) *(Golebiewski M., Boyd D., 2019)*.

4.

КОМПЈУТЕРСКИОТ КРИМИНАЛ И СОЦИЈАЛНИТЕ МРЕЖИ КАКО АЛАТКИ ЗА СТРАНСКО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Намерните обиди за манипулирање со информациите од страна на странски актери добиваат значителен поттик со технолошкиот напредок. Ширењето на социјалните платформи и комуникациските услуги овозможува поголем досег на странско мешање и манипулирање со информации, како и комбинација на нови и разновидни тактики, техники и процедури.

4.1. МЕЃУСЕБНА ПОВРЗАНОСТ НА САЈБЕР-НАПАДИТЕ И ДЕЗИНФОРМАЦИИТЕ ЗА МАНИПУЛАЦИЈА

Дезинформациите креирани од странски актери инкорпорирани во сајбер-напади се сметаат за значајни закани бидејќи можат да шират малициозен софтвер, да се мешаат во политичките процеси, да бидат тешки за откривање, да предизвикаат штета и да поттикнат насилство. Сајбер-криминалците собираат податоци преку таргетирани напади против институции, групи или поединци, но и ги користат за манипулација со информациите и нивно споделување. Случаите со хакирање и злоупотреба на одредени профили за да се обезбеди легитимност на специфична содржина или да се споделува наводен автентичен материјал се само некои од примерите што ја илустрираат врската помеѓу сајбер-безбедноста и манипулацијата со информацискатa средина.

Софистицираните малициозни кампањи ги комбинираат дезинформациите и сајбер-нападите преку:

- **Теренот** на кој се дистрибуираат дезинформациите (социјална мрежа, мрежна инфраструктура, услуги за пренасочување). За дезинформациите да можат да се шират и да допрат до целната публика, потребни се три фактори – социјални мрежи, алатки и услуги, и мотивација, а без кој било од нив не можат да бидат „успешни“. Алатките и услугите за манипулирање и ширење на пораките низ социјалните мрежи се продаваат во целиот свет. Некои се релативно еднотавни (платени лајкови, следбеници итн.), додека некои поневообичаени услуги се преку онлајн-анкети, или убедување на администраторите да направат отстранување или промена на некоја содржина. За овие алатки да бидат од корист, социјалните мрежи служат како платформа за ширење на дезинформациите. Со оглед на тоа што луѓето поминуваат повеќе време и почесто се информираат од социјалните платформи, нивната важност во ширењето лажни информации не може да се потцени. Сепак, постои разлика помеѓу едноставното објавување дезинформации и привлекувањето на целната публика да ги консумира. Оттука, спамерите користат различни техники за да ги намамат корисниците да ги консумираат нивните информации. Неодамнешните истражувања покажуваат дека веб-локациите за дезинформации често ги користат социјалните платформи како овозможу-

вачи, но се протегаат и надвор од нив, користејќи мрежна инфраструктура и услуги за пренасочување на различни нивоа на интернет. Конечно, зад дезинформациските кампањи секогаш постои прашањето „Зошто?“. Мотивацијата понекогаш едноставно е желба за парична добивка, а во други случаи може да варира од криминална до политичка.

- **Тактиките** што ги интегрираат дезинформациите како дел од пакетот на сајбер-напади. Дезинформациите станаа сè почеста компонента на сајбер-нападите, служејќи за испорака на малициозен софтвер преку искористување на емоциите и стравовите на луѓето. На пример, напаѓачите употребуваат „fearware“, подгрупа на измами за кражба на податоци познато како фишинг (phishing), кои се потпираат на вознемиреност и дезинформации, а кои станаа особено присутни за време на пандемијата на ковид-19 и по неа. Дополнително, постои значително преклопување на кампањите за дезинформирање и тактиките за сајбер-криминал, како што се нелегални трансакции на даркнет (дел од интернетот до кој се пристапува со користење посебен софтвер), употреба на нелегално добиени документи и различни форми на измама.

- **Целите** што доведуваат до тоа жртвите на сајбер-напади истовремено да бидат жртви на дезинформации. Дезинформациските кампањи и сајбер-нападите можат да предизвикаат слични видови штета, па дури може и да се комбинираат за да ги таргетираат истите жртви. Додека кражбата на податоци може да ја загрози безбедноста со изложување на чувствителни информации, манипулацијата со тие податоци исто така може да има слични ефекти.

- **Можностите,** т.е. профитабилните опции и за кампањи за дезинформирање и за сајбер-напади. Хакирањето, сајбер-криминалот и активностите за влијание често користат квалификувани професионалци како аутсорсинг, кои добиваат големи финансиски стимулации. Додека одбраната од напади може да се зајакне со разни комерцијални софтвери, стратегиите за дезинформирање можат да ги користат за нанесување штета врз угледот и за генерирање профит. Моментално нема сериозни казни за ваквите активности заради сложеноста на нивното истражување и недостигот од соодветни мерки за нивно ограничување и блокирање.

Дезинформациските кампањи најчесто се спроведуваат преку социјалните мрежи затоа што теоретски потешко може да бидат откриени од платформите за социјални медиуми, а секоја кампања опфаќа специфични алатки, како што се

купени следбеници, допаѓања, реобјавувања, коментари, видеа и сл. Голем дел од измамничките информации се изведени од теории на заговор или политички или групни идеологии. Такви примери се следните:

> За време на претседателската кампања во 2016 година Доналд Трамп објави статистика за криминал во САД според која процентот на белците убиени од белци бил 16%, а на белците убиени од црнци бил 81%, додека во реалноста бројките биле обратни, односно околу 16% од белците биле убиени од црнци.[7]

> Џејда Франсен, заменик-претседателка на британската десничарска партија Прво Британија, постираше видео со натпис: „Муслимански мигрант претепа холандско момче на патерици!“. Тогашниот американски претседател Трамп го споделува видеото, но набргу потоа холандската амбасада објавува со факти дека сторителот на насилниот чин на ова видео е по потекло од Холандија.[8]

> Нејчурал њуз (Natural News), веб-страница што вообичаено се занимава со теории на заговор, објави дека „Вакцините што содржат жива се ‘медицински геноцид’ што ги таргетира црните заедници за да им наштети на нивните бебиња“. Преку манипулација на вистинити написи, тие се обидуваа да влијаат на јавното мислење.[9]

7 Види повеќе на: https://www.washingtonpost.com/news/the-fix/wp/2015/11/22/trump-retweeted-a-very-wrong-set-of-numbers-on-race-and-murder/

8 Види повеќе на: https://www.pbs.org/newshour/politics/trump-retweets-anti-muslim-videos-from-british-far-right-leader

9 Види повеќе на: https://pmc.ncbi.nlm.nih.gov/articles/PMC9359307/

Сиетл трибјун (Seattle Tribune), веб-страница за лажни информации што презема и променува содржини од легитимни веб-страници, сподели лажна приказна за „мајка од Ајдахо осудена на затвор поради доење“. Оваа приказна беше споделувана на социјалните мрежи и ја раздвижува дискусијата околу доењето во јавноста.

Кампањите за дезинформација промовираа лажни вести дека 5Г-технологијата влијае на имунолошкиот систем и дека бендовите на спектарот 5Г шират ковид-19.[10]

Лажните информации за третманите за ковид-19 сè уште се шират на социјалните мрежи, од кои голем број даваат штетни предлози и дека користењето недозволени дроги може да го „излечи“ вирусот.[11]

4.2. КОМПЈУТЕРСКИОТ КРИМИНАЛ И ДЕЗИНФОРМАЦИИТЕ КАКО РИЗИК НА ЕКОНОМСКИОТ СЕКТОР

Лажните информации може да претставуваат значителни сајбер-ризици и за економскиот сектор, преку што може да се зголеми влијанието на лажната, променета информација доколку се однесува на повеќе области од општественото живеење. Вообичаени типови лажни информации и сајбер-ризици за кои компаниите треба да бидат свесни се:

10 Види повеќе на: https://www.bbc.co.uk/bitesize/articles/zbw492p

11 Види повеќе на: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en

- **е-пораки за фишинг (phishing),** т.е. е-пораки што изгледаат дека се од доверлив извор за да го измамат примачот да кликне на злонамерен линк или да преземе малициозен софтвер. Корисниците, исто така, може да бидат измамени да кликнат на малициозни линкови, да преземаат малициозен софтвер или да откриваат чувствителни информации преку објави на социјалните мрежи или други видови погрешни информации. Компаниите можат да го ублажат овој ризик со имплементирање силни безбедносни мерки за е-пошта, како што се филтри за спам и обука на вработените за тоа како да идентификуваат и да избегнуваат фишинг-пораки на своите е-пошти;

- **малициозен софтвер и злонамерен софтвер за заклучување на податоците (ransomeware),** кои се типови малициозен софтвер што може да зарази мрежа или уреди. Тука спаѓа манипулирање со визуелни знаци во корисничките интерфејси за да ги измамат корисниците да кликнат на копче или да внесат информации во форма. Откако ќе се инсталира, малициозниот софтвер може да украде податоци или да ги заклучи системите;

- **лажни веб-локации или профили на социјалните медиуми што содржат злонамерен софтвер.** Така, се користат лажни реклами за измамување на корисниците да преземаат малициозен софтвер на своите уреди. При тоа, се искористуваат човечките предрасуди, како што е тенденцијата да им се верува на авторитетите или да се следи толпата, за да се влијае врз носењето на одлуката да се посетат лажните веб-локации. Од тој аспект, компаниите треба да имплементираат силни протоколи за сајбер-безбедност, како што се автентикација со два фактори и ограничувања за пристап, firewall, антивирусен софтвер, редовни ажурирања на софтверот и обука на вработените за најдобри практики за сајбер-безбедност. Слични мерки на претпазливост може да се применат за да се избегне сајбер-шпионажа, каде што напаѓачите користат лажни информации за да соберат разузнавачки информации или да ја загрозат безбедноста;

- **напади од социјален инженеринг,** како што се кражба на податоци и кражба на идентитет, т.е. манипулирање со корисниците за откривање чувствителни информации, како што се податоците за најавување или финансиски податоци. Пример за ова е финансиска измама со која може да се промовираат лажни инвестициски шеми или измами со криптовалути, што ги наведува корисниците да испраќаат пари или криптовалути на лажни сметки. Ова може да се направи преку лажни телефонски повици, лажни страници за најавување, порака преку е-пошта за фишинг или пораки на социјалните мрежи што изгледаат дека се од

доверлив извор. За да се избегне социјален инженеринг, компаниите треба да обезбедат редовна обука на вработените за тоа како да ги идентификуваат и да ги избегнуваат таквите случаи.

4.3. МЕХАНИЗМИ ЗА САЈБЕР-БЕЗБЕДНОСТ И ЗАШТИТА ОД ДЕЗИНФОРМАЦИИ

Намерното ширење лажни информации со намера да се манипулира со јавното мислење или да се предизвика штета, обично претставени како кампањи за дезинформирање, може да ја наруши сигурноста и репутацијата на една институција, група или поединци.

> Владите, компаниите и корисниците стануваат сè посвесни за ваквите закани. Разни владини агенции сега поставуваат сервиси за разоткривање информации за кои сметаат дека се лажни. Тие, исто така, размислуваат да воведат регулативи и да ги казнат сајтовите што објавуваат дезинформации. Целите на новите регулативи ќе вклучуваат и можност за суспендирање на бот/сомнителни корисници и креирање сервиси што ќе им овозможат на корисниците да пријавуваат лажни информации. На крај, сепак, најважна е соодветната едукација на сите корисници како да ги идентификуваат лажните информации.

Потенцијалните одговори за справување со сајбер-заканите може да бидат:

- зголемување на улогата на сајбер-безбедноста во идентификацијата, истражувањето и превенцијата од странско мешање и манипулирање со информации;

- структурирано известување за инциденти помеѓу ентитетите одговорни за сајбер-безбедност и за странско мешање и манипулирање со информации;

- размена на информации и споделување на најдобрите практики;
- унапредување и олеснување на соработката помеѓу институциите и телата на ниво на држава;
- подигање на свеста и поддршка на градење капацитети.

Иако откривањето дезинформации може да биде комплексна задача, постојат одредени техники и тактики со кои може да се идентификуваат потенцијалните дезинформациски кампањи и да се преземат соодветни активности за ублажување на ризиците, како што се:

- поставување предупредувања на социјалните медиуми и други извори на вести за какви било знаци на ширење лажни информации, вообичаено преку користење клучни зборови и фрази што може да бидат поврзани со дезинформацијата;
- верификување на секоја информација што се шири преку проверка на веродостојноста на изворот и испитување на доказите што се презентирани за да се поддржат тврдењата што се дадени;
- ангажирање на сите засегнати страни за да се идентификуваат сите лажни информации што се шират и да се решат сите грижи или прашања што може да се појават;
- спроведување проценка на ризикот за да се оцени потенцијалното влијание на дезинформациската кампања, што ќе помогне да се подготви соодветен одговор;
- соработка со експерти за сајбер-безбедност, односи со јавноста и справување со кризи за ефикасно откривање, справување со ризиците и одговор на дезинформациската кампања.

4.4. СОВЕТИ ЗА ЗАШТИТА ОД САЈБЕР-ЗАКАНИ

Секој што е активен онлајн презема одреден ризик да добива или да пренесува лажни информации или да биде жртва на кражба на идентитет или друг тип злоупотреба или сајбер-криминал. Секоја информација што се објавува или се споделува на интернет никогаш не исчезнува, не може целосно да се отстрани и може да биде предмет или цел на злоупотреба. Иако се користат различни нагодувања на приватност, не мора да значи дека личните податоци секогаш се безбедни. Сето ова не само што може да ги доведе луѓето во онлајн- и физичка опасност, туку може и да биде искористено за креирање и ширење малициозни пораки и софтвери. Пример за тоа каде сајбер-криминалците често одат да дознаат важни информации за одредени лица е социјалната платформа Линкдин (LinkedIn). Оваа страница за социјално вмрежување може да му обезбеди на потенцијалниот криминалец имиња на вработени, работни позиции, работни обврски, па дури и колку долго работникот работел во организацијата. Овие информации потоа криминалците може да ги користат за да ги таргетираат вработените со „висок ризик“, па дури и да се користат како дел од поголема кампања за социјален инженеринг. Бидејќи сите овие информации сега се јавно достапни, луѓето треба да бидат свесни и едуцирани за ризиците при објавувањето и споделувањето информации, откривањето чувствителни детали за себе или за некоја организација и секако да умеат да одговорат на потенцијално злонамерни активности и социјален инженеринг.

Генерално, постојат два начини на кои хакерите и сајбер-криминалците го користат социјалниот инженеринг за да ги злоупотребат социјалните мрежи:

1. Обид да се натера некој да инсталира софтвер на компјутер или телефон што ќе му овозможи пристап до тој уред.

2. Да се стекне нечија доверба за различен вид манипулација преку социјалните мрежи.

Луѓето се најслабата алка во сајбер-безбедноста и секој хакер ќе го искористи тоа секогаш кога е можно. Ова се некои од најчестите начини што ги користат сајбер-криминалците:

- некористењето соодветни безбедносни сетирања на страниците на социјалните платформи. На пример, споделување локација, неограничување кој има пристап до одредени информации и сл.;

- објавување лични информации, банкарски или други финансиски податоци на социјалните мрежи, вклучувајќи датум на раѓање, телефонски број, адреса, банкарска сметка. Ако се разменуваат овие информации, тоа треба да биде преку приватни пораки или е-пошта;

- контакт од непознати лица од други држави. Честопати, измамниците се обидуваат да ја запознаат жртвата, а потоа ќе ја измамат. Ова често се случува со онлајн-страниците за запознавање. Тие може да користат социјален инженеринг за да убедат дека им требаат пари, но исто така може да ја искористат жртвата за ширење малициозен софтвер или лажни информации;

- со зголемувањето на популарноста на услугите за приватни пораки што се дел од социјалните медиуми, како што е Фејсбук месинџер (Facebook Messenger), се испраќаат приватните пораки со линк без објаснување или имаат нејасен опис за тоа што може да содржи линкот;

- нудење нереална понуда. Сајбер-криминалците користат популарни настани и вести како мамка за да ги натераат луѓето да отворат заразена е-пошта, да посетуваат заразени веб-страници, да донираат во лажни добротворни организации или да купат предмети што или не постојат или се фалсификувани;

- неменување на лозинките за социјалните мрежи. Истражувањата покажуваат дека голем број злоупотреби се поради повторната употреба на лозинки и украдени податоци за најава – 53 % од корисниците на социјалните мрежи не ги промениле лозинките повеќе од една година, а 20 % никогаш не ги сменило. Препорачливо е тоа да се прави почесто.

Конечно, само со подигнување на јавната свест и медиумската и информациската писменост на граѓаните може да се постигне правилно користење на социјалните платформи и мрежната инфраструктура и добра проценка на содржините, за да се превенираат злоупотреба и манипулација со информациите.

5.

КРАТОК ОСВРТ НА ЕВРОПСКИТЕ ДОБРИ ПРАКТИКИ ВО СПРАВУВАЊЕТО СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

За да се даде патоказ како Северна Македонија би можела да се справи со странското мешање и манипулирање со информации, во оваа студија се нуди краток преглед на добрите европски практики. Тоа треба да биде дополнителен поттик, но и рамка што ќе овозможи целисходен пристап кон овој феномен и намалување на притисокот од СММИ што ги загрозува демократскиот процес, институционалната стабилност и јавниот дискурс.

5.1. УСПЕШНИ ПРАКТИКИ ВО ДЕЛ ОД ЗЕМЈИТЕ ОД ЕУ

Она што ги издвојува успешните држави во оваа област е нивниот систематски и мултидимензионален пристап, кој опфаќа три клучни аспекти: (1) регулаторна рамка, (2) институционален капацитет и (3) јавна свест и медиумска и информациска писменост. Овој пристап овозможува поефикасно справување со странското мешање и манипулирање со информации преку превенција, рано откривање и брз институционален одговор.

5.1.1. ЈАКНЕЊЕ НА ИНСТИТУЦИОНАЛНИОТ ОДГОВОР: УСПЕШНИ МОДЕЛИ

Во земјите што успеале да изградат ефикасен одбранбен механизам против странското мешање и манипулирање со информации, институциите играат клучна улога не само во мониторингот, туку и во активното разобличување на дезинформациите.

Финска, на пример, е позната по својот сеопфатен модел на одбрана, каде што безбедносните агенции, медиумите, граѓанските организации и образовните институции тесно соработуваат. Владата на Финска, преку Агенцијата за безбедност и снабдување (Huoltovarmuuskeskus - HFK), редовно изработува ризични проценки и стратегии за справување со странските информативни закани. Овој модел покажува дека една од клучните точки за градење општествена еластичност е константната анализа и информирање на јавноста за потенцијални закани.

Сличен пристап применува и Шведска, која во 2022 година го формираше Центарот за психолошка одбрана (MPF). Ова тело има задача активно да следи, да анализира и да дава препораки за справување со странските информативни напади. Со оглед на тоа што во Северна Македонија недостигаат координиран институционален одговор и посебна единица што систематски се занимава со странското мешање и манипулирање со информации, овој модел може да биде особено значаен.

Од друга страна, Чешка, по искуството со засилените дезинформациски кампањи во 2017 година, основаше специјална единица за борба против хибридни закани во рамките на Министерството за внатрешни работи. Оваа единица е составена од експерти од различни области, меѓу кои претставници на разузнавачките служби, новинари, ИТ-безбедносни експерти и психолози. Ваквиот пристап кон операциите за влијание или хибридните закани дава различни перспективи кон еден ист проблем, што ѝ овозможува на Чешка да даде брз и ефективен одговор на дезинформациите и другите облици на странско штетно влијание.

За Северна Македонија, овие модели укажуваат на неопходноста од посебна институционална структура, која ќе биде одговорна за мониторинг, анализа и реакција на дезинформациите. Оваа институција би требало да има мандат и за соработка со медиумите и граѓанските организации.

5.1.2. РЕГУЛАТОРНА РАМКА: КАКО ПРАВОТО МОЖЕ ДА ЈА ЗАШТИТИ ДЕМОКРАТИЈАТА?

Освен институционалниот капацитет, регулативата игра клучна улога во ограничувањето на влијанието на странското мешање и манипулирање со информации. Во повеќе европски земји законите се изменети за да ја зголемат транспарентноста на медиумското финансирање, да постават јасни критериуми за работата на социјалните мрежи и да ги санкционираат оние што намерно шират дезинформации.

Во Франција, на пример, во 2018 година беше донесен Законот за манипулација на информации, кој на државните институции им овозможува да бараат од социјалните платформи, како Фејсбук и Икс, да отстранат лажни содржини за време на избори. Со ова, дезинформациските кампањи немаат доволно време да се прошират и да влијаат врз гласачкото тело.

Во Литванија, пак, е во сила закон што го ограничува емитувањето странски медиуми доколку тие се идентификувани како пропагандни алатки. Владата обезбедува финансиска поддршка за независните медиуми, со што ја намалува нивната зависност од надворешни извори на финансирање што може да бидат политички мотивирани, односно да паднат во замката на искористување на отворените општества и затскривање на странски служби зад лукративни финансиски инвестиции.

Северна Македонија во овој контекст треба да размисли за законска рамка што ќе ја зголеми транспарентноста на медиумската сопственост, особено на онлајн-порталите, ќе ги зајакне капацитетите за мониторинг на онлајн-пропагандата, ќе даде придонес кон одржливоста и независноста на медиумите и ќе предвиди посебни механизми за справување со дезинформациите во пресрет на избори.

5.1.3. ЈАВНАТА СВЕСТ И МЕДИУМСКАТА ПИСМЕНОСТ: КЛУЧНА ЛИНИЈА НА ОДБРАНА

Како што покажуваат искуствата на Финска и Летонија, една од најсилните заштити од странското мешање и манипулирање со информации е образованието. Финска ја воведе медиумската писменост како задолжителен дел од образовниот систем, а професорите добиваат специјализирани обуки за да ги едуцираат и да ги образуваат учениците како да анализираат вести, информации и да ги препознаваат манипулативните техники. Во Летонија, пак, државата финансира национални кампањи за медиумска писменост, кои вклучуваат онлајн-предавања, видеоматеријали и работилници за новинари, наставници и студенти.

Во Северна Македонија на ова поле сè уште има простор за развој. Пристапот кон јакнење на националната свест се сведува генерално на медиумската писменост и главно зависи од иницијативите на граѓанскиот сектор, односно донаторите. Доколку државата го следи примерот на Финска, медиумската писменост може да стане системски механизам за намалување на подложноста на дезинформации, а со тоа и на странското манипулирање и влијание, тренд специфичен особено кај младата популација.

***

Сепак, во примената на овие мерки Северна Македонија мора да внимава на демократскиот баланс помеѓу индивидуалните права и јавната безбедност и добро. Примената на дел од овие мерки лесно може да има сосема спротивен ефект. Неправилната имплементација на ваквите мерки може да доведе до загрозување на слободите и правата и да биде основа за апсолутизам. Францускиот Закон за манипулација на информации, на пример, иако овозможува брзо отстранување лажни информации, истовремено создава можност за селективна цензура, особено доколку институциите што ја контролираат оваа регулација се под политичко влијание. Во Северна Македонија постои ниско ниво на доверба во институциите и сериозна политизација на речиси секој сектор, што го зголе-

мува ризикот ваквите механизми да се користат како алатка за сузбивање на политичките неистомисленици наместо за вистинско спротивставување на странското мешање и манипулирање со информации.

Дополнително, моделите што вклучуваат државно регулирање на медиумскиот простор, како оној во Литванија, каде што се забрануваат одредени медиуми заради заштита од пропаганда, може да предизвикаат спротивен ефект. Така, во случај на политички инженеринг од владејачката гарнитура, довербата во институциите наместо да се зајакне, може лесно да се намали или да се загуби. Ако се намали транспарентноста или ако се прави партиска селекција, граѓаните, заедно со опозицијата, лесно може да ги перципираат ваквите мерки како цензура. Во Северна Македонија, каде што јавноста веќе е скептична кон владините политики во медиумскиот сектор, воспоставувањето механизми за ограничување на одредени извори може да доведе до дополнителна поларизација и да создаде простор за алтернативни, уште порадикални дезинформациски канали. Токму таквиот исход би можел да ја засили кампањата на влијание и да го подгрее целиот информациски хаос, во кој преку странско мешање и манипулирање со информации ќе се влијае на подривање на вербата во демократските процеси и институции, а лошите практики на владејачките елити ќе се изедначат со политиките на ЕУ и НАТО.

Конечно, создавањето централно тело за борба против дезинформациите, доколку не е доволно независно и транспарентно, може само да генерира нова точка на странско мешање и манипулирање со информации. Ако Северна Македонија не внимава на институционалната непристрасност, тогаш наместо ваквите механизми да помогнат во намалување на влијанието на дезинформациите, тие може да станат уште еден извор на недоверба, дополнително комплицирајќи ја борбата против СММИ. За да се избегне овој ризик, неопходно е овие политики да бидат развиени преку широк консултативен процес со експерти, медиуми и со граѓанското општество, наместо да бидат исклучиво под капата на државните институции.

5.2. КРАТОК ПРЕГЛЕД НА ДОБРИТЕ ПРАКТИКИ И ИСКУСТВАТА НА ЕУ И НАТО ВО СПРАВУВАЊЕТО СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ

Во последните години ЕУ и НАТО станаа свесни за сериозните последици од странското мешање и манипулирање со информации врз нивната безбедност, политичка стабилност и демократски процеси. Хибридните закани, особено дезинформациските кампањи предводени од странски државни и недржавни актери, бараа системски и координиран одговор. Како резултат на тоа, се развија неколку клучни механизми за справување со СММИ, кои денес се меѓу најуспешните примери во глобалниот одговор на информативните закани. Во оваа студија се нуди осврт на три од најзначајните иницијативи: Наменските сили за стратегиска комуникација – Исток на ЕУ (East StratCom Task Force) (ЕУ), Центарот за извонредност за хибридни закани (Hybrid Center of Excellence) (Финска) и Системот за брзо предупредување на ЕУ (Rapid Alert System) (ЕУ), и се истакнуваат лекциите што Северна Македонија може да ги извлече од нив.

5.2.1. НАМЕНСКИТЕ СИЛИ ЗА СТРАТЕГИСКА КОМУНИКАЦИЈА - ИСТОК НА ЕУ (EAST STRATCOM TASK FORCE)

Наменските сили за стратегиска комуникација - Исток на ЕУ (East StratCom Task Force) е првиот организиран фронт против дезинформациите. Формиран во 2015 година во рамките на Европската служба за надворешни работи (European Union External Action - EEAS), тој претставува првиот обид на ЕУ за систематско справување со дезинформациите, особено со оние што доаѓаат од Руската Федерација. Главна цел на ова тело е да ги идентификува, анализира и да ги разобличува дезинформациските наративи, но и да ги зајакне комуникациските капацитети на ЕУ во источното соседство.

Овој механизам се потпира на три столба на дејствување, и тоа:

1. Проактивна комуникација на ЕУ во источното соседство – преку креирање и дистрибуција на коректни и проверени информации, East StratCom работи на јакнење на позитивниот наратив за ЕУ. Ова особено се однесува на земји како Украина, Грузија и Молдавија, кои често се цел на анти-ЕУ пропаганда.

2. Следење и разобличување на дезинформациите – тимот управува со платформата EUvsDisinfo, која ги следи и ги разобличува дезинформациските наративи. Преку детална анализа, платформата ги етикетира лажните информации, објаснува како се шират и дава фактички исправки.

3. Јакнење на медиумската писменост и отпорноста на општествата - East StratCom соработува со локални медиуми, граѓански организации и експерти, нудејќи обуки за проверка на факти, аналитички алатки и насоки за откривање дезинформации.

Од овој механизам на ЕУ како клучни лекции за Северна Македонија се издвојуваат:

- потребата за координиран пристап меѓу државните институции и невладиниот сектор за следење на дезинформациите;

- развој на национална платформа за разобличување на манипулациите и мешање преку странски информации (слична на EUvsDisinfo); и

- инвестирање во професионално комуницирање на државните институции за да се намали просторот за манипулација.

5.2.2. ЦЕНТАР ЗА ИЗВОНРЕДНОСТ ЗА ХИБРИДНИ ЗАКАНИ (HYBRID CENTER OF EXCELLENCE): ХИБРИДНА ОДБРАНА ПРЕКУ СТРАТЕГИСКА АНАЛИЗА И КООРДИНАЦИЈА

Центарот за извонредност за хибридни закани (Hybrid CoE), основан во Финска во 2017 година, претставува еден од најкомплексните обиди за справување со хибридните закани, вклучувајќи странско мешање и манипулирање со информации. Овој центар функционира како платформа за споделување информации, анализи и експертиза помеѓу земјите членки на НАТО и ЕУ. За разлика од East StratCom, кој

е насочен кон конкретни дезинформации, Центарот за извонредност за хибридни закани има поширока мисија, анализирајќи ги сите аспекти на хибридните закани, како што се економските притисоци, сајбер-нападите и изборните манипулации. Центарот работи преку три главни платформи, и тоа:

1. Анализа на хибридните закани и странското мешање и манипулирање со информации – Центарот објавува детални студии и предвидувања за тоа како се развиваат дезинформациските стратегии и хибридните закани.

2. Тактички симулации и сценарија – Центарот организира тренинг-сесии за влади, медиуми и безбедносни агенции, со цел да ги подготви за потенцијални информативни напади.

3. Градење стратегиски капацитети - поддршка за земјите во развивањето национални стратегии за хибридна одбрана, вклучувајќи мерки за спречување на СММИ.

Клучни лекции за Северна Македонија во однос на Центарот за извонредност за хибридни закани се:

- развој на национален центар за хибридни закани, кој ќе го анализира странското мешање и манипулирање со информации во поширок контекст;

- организирање вежби за институциите засновани на можни сценарија, како подготовка за информативни напади; и

- зголемување на регионалната соработка со НАТО и ЕУ во областа на хибридната одбрана.

5.2.3. СИСТЕМ ЗА БРЗО ПРЕДУПРЕДУВАЊЕ НА ЕУ (RAPID ALERT SYSTEM): БРЗ ОДГОВОР НА ИНФОРМАТИВНИТЕ ЗАКАНИ

Во 2019 година ЕУ го воспостави Системот за брзо предупредување на ЕУ (Rapid Alert System - RAS) како дел од стратегијата за заштита од странско мешање во изборите и политичките процеси. Овој систем овозможува брза размена на информации меѓу земјите членки, заради идентификација и ограничување на дезинформациските кампањи во реално време.

Системот работи на следниов начин:

- државите членки веднаш разменуваат податоци за идентификувани дезинформациски операции;
- се користат напредни дигитални алатки за следење на социјалните мрежи и сајтовите што шират дезинформации;
- информациите се споделуваат со платформите како Фејсбук, Икс и Јутјуб, кои имаат обврска да постапат според заклучоците на Системот за брзо предупредување на ЕУ (RAS).

Добрите практики што може да се применат во Северна Македонија се:

- воспоставување интериснтитуционален механизам за брза размена на информации за странско мешање и манипулирање со информации;
- зајакнување на соработката со глобалните платформи за да се намали дезинформациското влијание во онлајн-просторот; и
- развој на локален мониторинг систем што ќе обезбедува рано предупредување за потенцијални дезинформациски кампањи.

ПРЕПОРАКИ ЗА КРЕИРАЊЕ ПОЛИТИКИ ЗА СПРАВУВАЊЕ СО СТРАНСКОТО МЕШАЊЕ И МАНИПУЛИРАЊЕ СО ИНФОРМАЦИИ ВО СЕВЕРНА МАКЕДОНИЈА

За ефективно справување со странското мешање и манипулирање со информации, потребен е холистички пристап што ќе ги опфати институционалните, регулаторните и општествените аспекти на оваа закана. Следните препораки за креирање политики се насочени кон зајакнување на националната отпорност и намалување на влијанието на дезинформациите врз безбедноста, медиумскиот простор и јавниот дискурс.

1. ИНСТИТУЦИОНАЛНО ЗАЈАКНУВАЊЕ И КООРДИНАЦИЈА

- Воспоставување Национален центар за мониторинг и анализа на странското мешање и манипулирање со информации, кој ќе ги обедини институционалните напори за следење, истражување и реагирање на странските дезинформациски операции.

- Формирање интеринституционална работна група со претставници од Владата, безбедносните служби, медиумските регулатори и граѓанскиот сектор за редовно разменување информации и најдобри практики.

- Подобрување на механизмите за кризни комуникации, особено во случаи на зголемени дезинформациски кампањи поврзани со избори, националната безбедност или здравствени и социјални прашања.

- Унапредување на капацитетите на безбедносните институции за разузнавачка анализа на дезинформациите и развој на алатки за откривање организирани кампањи.

- Деполитизација на јавната администрација и безбедносниот сектор и јакнење на интегритетот во управувањето со државните органи и органите на упра-

вата преку професионален, одговорен и транспарентен пристап во склад со демократските принципи на владеење.

2. ЗАКОНСКИ И РЕГУЛАТОРНИ МЕРКИ

- Ревидирање на постоечките законски рамки за дезинформациите, со јасно дефинирање на границата помеѓу слободата на изразување и штетната манипулација со информации.
- Зајакнување на надзорот врз онлајн-платформите преку зголемена транспарентност на финансирањето и политичкото рекламирање.
- Обврска за идентификација на изворите на финансирање на медиумите, со цел да се спречат странски влијанија преку онлајн медиумите или прикриени мрежи на дезинформација.
- Интеграција на европските и НАТО-препораките за борба против дезинформациите во националната регулатива, усогласување со Акцискиот план на ЕУ против дезинформации и подобрување на механизмите за отчетност.

3. ЈАКНЕЊЕ НА МЕДИУМСКАТА ОТПОРНОСТ И ТРАНСПАРЕНТНОСТ

- Поддршка за развој на независни центри за проверка на факти, кои ќе соработуваат со медиумите и ќе имаат официјална улога во разобличувањето на дезинформациските кампањи.
- Зголемување на транспарентноста во работата на медиумите, преку обврски за обелоденување на сопственоста и надзор врз финансирањето на онлајн-платформите.
- Унапредување на јавниот сервис и независните медиуми преку промовирање на професионалното новинарство и спротивставување на ширењето на дезинформациите.

4. ГРАДЕЊЕ ОПШТЕСТВЕНА ОТПОРНОСТ И МЕДИУМСКА ПИСМЕНОСТ

- Одржување и унапредување на медиумската и информациската писменост во образовниот систем преку едукативни програми за ученици и студенти за критичко размислување и справување со дезинформациите.

- Поддршка за јавните кампањи против дезинформации, кои ќе ги едуцираат граѓаните за техниките на манипулација со информации и за важноста на проверката на изворите.

- Стимулирање истражувања и академски анализи за развој на стратегии за борба против странското мешање и манипулирање со информации, со посебен акцент на локалниот контекст и специфичните ранливости на Северна Македонија.

5. ЗГОЛЕМУВАЊЕ НА МЕЃУНАРОДНАТА СОРАБОТКА

- Продлабочување на партнерството со НАТО и ЕУ преку учество во заеднички иницијативи за размена на податоци, разузнавачка анализа и стратегии за борба против странското мешање и манипулирање со информации.

- Јакнење на соработката со меѓународни организации и истражувачки центри, како што се НАТО-центарот за извонредност за стратегиски комуникации (StratCom CoE), Центарот за извонредност за хибридни закани (Hybrid CoE) и Наменските сили за стратегиска комуникација Исток на ЕУ (East StratCom Task Force), за добивање пристап до аналитички алатки и методологии.

- Развивање регионални механизми за размена на информации со соседните земји, бидејќи странското мешање и манипулирање со информации често ги надминува националните граници и има транснационални импликации.

Овие препораки имаат цел да создадат поцврста основа за заштита на македонското општество од странските манипулативни влијанија и дезинформации. Преку стратегиски пристап што вклучува институционално зајакнување, законски реформи, медиумска отпорност, јавна едукација и меѓународна соработка, државата може да ја намали ранливоста на странското мешање и манипулирање со информации и да го зајакне демократскиот капацитет за одбрана од хибридни закани.

ЗАКЛУЧОК

Странското мешање и манипулирање со информации (СММИ) претставуваат значајна закана за националната безбедност, демократските процеси и јавната доверба во Северна Македонија. Како земја членка на НАТО и кандидат за членство во ЕУ, државата е изложена на различни облици на хибридни закани, вклучително и организирани дезинформациски кампањи, медиумска манипулација и сајбер-напади, кои имаат цел да ги поткопаат нејзините институции, да ја зголемат политичката поларизација и да го ослабат нејзиниот стратегиски правец кон евроатлантските интеграции.

Оваа студија ги идентификуваше клучните методи што ги користат различни актери за влијание врз македонското информативно опкружување, вклучувајќи создавање и ширење лажни наративи, злоупотреба на дигиталните медиуми и координирани кампањи насочени кон специфични општествени групи. Студијата посочува дека странското мешање и манипулирање со информации влијае врз повеќе сфери – општествената, медиумската и сајбер-сферата, и дека постојат системски ранливости што овозможуваат ваквите закани да бидат ефективни. Недоволната медиумска писменост, ниското ниво на доверба во институциите, недостигот од механизми за брза реакција и ограничените капацитети за следење и анализа на дигиталните простори претставуваат критични точки што се искористуваат во овие манипулативни процеси.

Постоечките политики и регулаторни рамки во НАТО и ЕУ овозможуваат насоки и механизми за справување со СММИ, но нивната имплементација во Северна Македонија сè уште е во развој и бара дополнително унапредување. Споредбената анализа покажа дека некои земји во ЕУ имаат воспоставено поефикасни модели за справување со странските информативни манипулации, што може да послужи како пример за градење поотпорен институционален и општествен механизам.

Заради зајакнување на националната отпорност кон странското мешање и манипулирање со информации, оваа студија препорачува мултидимензионален пристап што вклучува зајакнување на институционалните капацитети за детекција и одговор на дезинформациите, деполитизација на професионалниот безбедносен сектор и јавната администрација, подобрување на регулативите за отчетност, транспарентност и интегритет на медиумите, како и подигнување на јавната свест преку едукација за медиумска и информациска писменост. Исто така, од

особено значење е засилената соработка со меѓународните партнери, особено со НАТО и ЕУ, заради споделување информации, добри практики и технички капацитети за справување со овој тип хибридни закани.

Северна Македонија се соочува со комплексен и динамичен предизвик кога станува збор за странското мешање и манипулирање со информации, но со соодветни стратегиски политики, институционални реформи и засилена јавна свест земјата може да го намали влијанието на странските манипулативни операции и да изгради поотпорно демократско општество. Борбата против дезинформациите и хибридните закани не е само безбедносно прашање, туку и клучен елемент за заштита на демократските вредности и на евроатлантската иднина на државата.

ЗА АВТОРИТЕ

Д-р Методи Хаџи-Јанев е вонреден професор на Правниот факултет при Универзитетот „Гоце Делчев“ – Штип и Воената академија „Генерал Михаило Апостолски“ – Скопје, како и гостин-професор на Инженерскиот факултет „Ира А. Фултон“ при Универзитетот Аризона Стејт, САД. Со меѓународно искуство во настава и консултантски активности, неговата експертиза опфаќа дигитално владеење, управување со ризик и усогласеност, сајбер безбедност и сајбер криминал, заштита на податоци, е-трговија и користење на технолошки алатки и платформи за унапредување на транспарентноста, отчетноста, ефективноста, ефикасноста и доброто владеење. Хаџи-Јанев бил вклучен како експерт во бројни регионални иницијативи (во Југоисточна Европа, вклучително и Молдавија и Грузија) и меѓународни организации, како што се УСАИД, Стејт департментот на САД, ЕУ, НАТО, RCC (со седиште во Сараево) и RACVIAC (со седиште во Загреб), фокусирајќи се на градење капацитети, вклучување на засегнатите страни и имплементација на стратегии за управување, ризик и усогласеност. Неговата работа ги поврзува јавниот, академскиот и приватниот сектор со цел поттикнување на добро владеење, транспарентност и дигитални иновации. Исто така, тој е вклучен во евалуација на високо ниво во институции како Европската комисија, Европската научна фондација и Словачката агенција за истражување и развој, и придонесува во Мрежа за глобална безбедносна евалуација предводена од Харвард.

Д-р Марјан Стоилковски, е раководител на Служба за ИТ безбедност во НЛБ Банка, а претходно 15 години беше началник на Секторот за компјутерски криминал и дигитална форензика во Министерството за внатрешни работи. Повеќе од 13 години работи како меѓународен експерт за сајбер безбедност, компјутерски криминал, дигитална форензика и електронски докази. Има спроведено повеќе од 80 меѓународни активности за јакнење на капацитетите за компјутерска безбедност и компјутерски криминал како дел од проектни активности на Советот на Европа, Европската комисија, Обединетите нации, ОБСЕ и други меѓународни институции и организации. Во моментот, неговиот научен и професионален фокус е во делот на сајбер безбедност односно имплементација на безбедносни решенија и тестирање, подготовка и реализација на практични Tabletop Exercises, управување со инциденти и дигитална форензика, SOC Managed services и malware analyses. Дополнителните истражувања вклучуваат Virtual assets во однос на анализа и регулација, OSINT и отворени извори на информации (и DARKNET) и користење на ВИ во оперативни активности за сајбер безбедност.

КОРИСТЕНА ЛИТЕРАТУРА

- Association of Journalists of Macedonia (2023). Media Freedom in North Macedonia: Fragile Progress, достапно на: https://znm.org.mk/wp-content/uploads/2023/10/%D0%9C%D0%9A-Fact-Finding-PFM-Report-251023-web.pdf
- BBC. 5G and coronavirus: Debunking the fake news stories, достапно на: https://www.bbc.co.uk/bitesize/articles/zbw492p
- BIRN Macedonia (2023). Media Ownership Monitor – North Macedonia, достапно на: https://north-macedonia.mom-gmr.org/mk/
- Blue Europe (2024). Challenges of Chinese Soft Power in Western Balkans, достапно на: https://www.blue-europe.eu/analysis-en/short-analysis/challenges-of-chinese-soft-power-in-western-balkans/
- Boulianne Sh., Humprecht E, (2023), Perceived Exposure to Misinformation and Trust in Institutions in Four, Countries Before and During a Pandemic, International Journal of Communication 17, достапно на: https://hal.science/hal-04126541/document
- CERT – EU (2024), Threat Landscape Report 2023, available at: https://cert.europa.eu/publications/threat-intelligence/tlr2023/
- Corporate Finance Institute (2023), Platform Company, достапно на: https://corporatefinanceinstitute.com/resources/valuation/platform-company/
- CSIS, (2021), Reimagining U.S. Policy toward the Western Balkans, достапно на: https://www.csis.org/programs/europe-russia-and-eurasia-program/archives/european-security-politics-and-economics-1
- Diamond L., McDonald J. (1996). Multi-Track Diplomacy: A Systems Approach to Peace. Third Edition. West Hartford, CT: Kumarian Press.
- Disinformation. достапно на: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
- Deutsche Welle (2024), „What is foreign information manipulation and interference?", достапно на: https://akademie.dw.com/en/what-is-foreign-information-manipulation-and-interference/video-68790017
- EU COMMISSION STAFF WORKING DOCUMENT, North Macedonia 2023 Report, достапно на: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf
- EU Commission, NIS2 Directive: new rules on cybersecurity of network and information systems, достапно на: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- EU Commission, (Brussels, 8.11.2023), North Macedonia 2023 Report, Commission Staff Working Document, достапно на: https://enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_693%20North%20Macedonia%20report.pdf

- EUEA (2023), 1st EEAS Report on Foreign Information Manipulation and Interference Threats, The Diplomatic Service of the European Union, достапно на: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
- EUEA (2025), Inside the infrastructure of Foreign Information Manipulation and Interference (FIMI) operations, достапно на: https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en
- European Commission. Separating facts from fiction on vaccines, достапно на: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en
- Golebiewski M., Boyd D. (2019). Data Voids: Where Missing Data Can Easily Be Exploited. Data & Society, достапно на: https://datasociety.net/library/data-voids/ https://www.facebook.com/photo
- Hubervic A., Prudent Y., for Enabling Alliance Interoperability and Pervasive M&S Applications. NATO Science and Technology Organisation (STO), достапно на: линк
- Jakov Marusic S., (2022). Forget Sputnik. Russian Propaganda Has other Paths into North Macedonia, BIRN, достапно на: https://balkaninsight.com/2022/04/22/forget-sputnik-russian-propaganda-has-other-paths-into-north-macedonia/
- Kelly S, Truong M., Shahbaz A., Earp M., White J. (2017). Manipulating Social Media to Undermine Democracy, Freedom House, достапно на: https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy
- Koldomasov A., Pylypenko A., (2024). How Russia Uses Propaganda To Hinder the Integration of Western Balkan Countries Into the EU. Detector media, достапно на: https://en.detector.media/post/how-russia-uses-propaganda-to-hinder-the-integration-of-western-balkan-countries-into-the-eu
- Miguel R., (2024). Decoding FIMI: a complex interrelation with disinformation, The ATHENA Newsletter, достапно на: https://project-athena.eu/decoding-fimi-a-complex-interrelation-with-disinformation/
- PBS News (2017). Trump retweets anti-Muslim videos from British far-right leader, достапно на https://www.pbs.org/newshour/politics/trump-retweets-anti-muslim-videos-from-british-far-right-leader
- Reporters Without Borders (2024). From Russia to Serbia: How RT Spreads the Kremlin's Propaganda in the Balkans Despite EU Sanctions, достапно https://rsf.org/en/russia-serbia-how-rt-spreads-kremlin-s-propaganda-balkans-despite-eu-sanctions
- Skafle I., Nordahl-Hansen A., Quintana D., Wynn R., Gabarron E. (2022). Misinformation About COVID-19 Vaccines on Social Media: Rapid Review. Journal of Medical Internet Research, достапно на: https://pmc.ncbi.nlm.nih.gov/articles/PMC9359307/
- Stanicek B. Caprile A., (2023). Russia and the Western Balkans Geopolitical confrontation, economic influence and political interference. European Parliamentary Research Service, достапно на: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/747096/EPRS_BRI(2023)747096_EN.pdf
- The Cybersecurity and Infrastructure Security Agency (CISA) (2023). Tactics of

- The Cybersecurity and Infrastructure Security Agency (CISA) (2023). Tactics of Disinformation. достапно на: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
- The Diplomatic Service of the European Union, (2025) „Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)" достапно на: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
- Tuneva M. (2023). „Between challenges and solutions - A Guide to Media Integrity in North Macedonia", UNDP, достапно на: https://dksk.mk/wp-content/uploads/2024/01/Media_Integrity_Guide_en-final.pdf
- Vatsov D., Dimitrova V., Donchev Lj., Valkanov V., Iakimova M, (2023). The Pro-Russian Propaganda Machine in Bulgaria, and the Russian Style Representations of North Macedonia. Identities: Journal for Politics, Gender and Culture, достапно на: https://identitiesjournal.edu.mk/index.php/IJPGC/article/view/530ч
- Walker Sh., Simeone M. (2020), Misinfo, Bots, and Trolls - Some Key Concepts for Misinformation, ASU Podcast, S1.E6, достапно на: https://lib.asu.edu/misinfo-weekly/misinfo-bots-and-trolls-some-key-concepts-misinformation
- Washington Post (2015). Donald Trump retweeted a very wrong set of numbers on race and murder, достапно на: https://www.washingtonpost.com/news/the-fix/wp/2015/11/22/trump-retweeted-a-very-wrong-set-of-numbers-on-race-and-murder/
- Агенција за аудио и аудиовизуелни услуги (ААВМУ). Мрежа за медиумска писменост - https://mediumskapismenost.mk/
- Анализа на профили активни на социјалните медиуми. На пример, „По патот на Македонија" (11 јануари 2025 година), достапно на:
- „Службен весник на Република Северна Македонија" бр. 152/2019 и 275/2019)
- Вистиномер, (2023). Путин на Црвениот плоштад ги повтори главните дезинформациски наративи – Русија е жртва и се бранела!, достапно на: https://vistinomer.mk/putin-na-crveniot-ploshtad-gi-povtori-glavnite-dezinformaciski-narativi-rusija-e-zhrtva-i-se-branela/
- Влада на Република Северна Македонија (2024), достапно на: https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=51471
- Влада на Република Северна Македонија, (2021), „Стратегијата за градење национална отпорност и справување со хибридни закани", достапна на: https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf
- Европска комисија, Работен документ на службите на Комисијата, Извештај за Северна Македонија за 2021 година, Стразбур, 19.10.2021 година, Собрание на РСМ
- EEA (2023). „Beyond Disinformation - What is FIMI?", достапно на: https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en#:~:text=Tackling%20Disinformation%2C%20Foreign%20Information%20Manipulation,democratic%20processes%2C%20security%20and%20citizens
- Закон за електронските комуникации („Службен весник на Република Македонија" бр. 39/2014), 188/2014, 44/2015, 193/2015, 11/2018 и 21/2018 и „Службен весник на Република Северна Македонија" бр. 98/2019 и 153/2019

- Закон за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20)
- Закон за изменување и дополнување на законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 294/21)
- Закон за кривична постапка („Службен весник на Република Северна Македонија“ бр. 150/10, 100/12, 142/16 и 198/18)
- Закон за правда за децата („Службен весник на Република Македонија“ бр. 148/2013 и „Службен весник на РСМ, бр. 66 од 20.3.2024 година“)
- Закон за следење на комуникациите („Службен весник на Република Северна Македонија“ бр. 71/18)
- Законот за аудио и аудиовизуелни медиумски услуги (пречистен текст) (Сл. весник бр. 184/2013, Сл. весник бр. 13/2014 и Сл. весник бр. 44/2014), достапен на: Zakon-za-Audio-i-audiovizuelni-mediumski-uslugi-prechisten-tekst-na-memorandum.pdf
- Законот за заштита на децата, „Службен весник на Република Македонија“ бр. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 и 198/2018 и „Службен весник на Република Северна Македонија“ бр. 104/2019, 146/2019, 275/2019, 311/2020 и 294/2021)
- Институт за комуникациски студии (2023). Ранливост на дезинформации кај различни групи граѓани во Северна Македонија. Рес публика, достапно на: https://iks.edu.mk/istrazuvanja-analizi/ranlivost-na-dezinformacii-kaj-razlichni-grupi-gragjani-vo-severna-makedonija/
- Институт за комуникациски студии (2024). Практики и перцепции на граѓаните во поглед на информирањето и справувањето со дезинформациите. Рес публика, достапно на: https://iks.edu.mk/istrazuvanja-analizi/praktiki-i-percepcii-na-gragjanite-vo-pogled-na-informiranjeto-i-spravuvanjeto-so-dezinformaciite/
- Јакимова Ј., (2022), „Кога се нема доверба во државата - се трупа масло и се одбиваат вакцини“, Радио Слободна Европа, достапно на: линк
- Клинчарски П., Гаџовска Спасовска З. (2024), Државни пари за невладини во рацете на дел од административците на ДУИ, Радио Слободна Европа, достапно на: https://www.slobodnaevropa.mk/a/drzhavni-pari-za-nevladini-vo-racete-na-del-od-administrativcite-na-dui/32788912.html
- Кривичен законик („Службен весник на Република Северна Македонија“ бр. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018 и број 36/23
- МИА, (9 април, 2022), „Петровска: Ниту една стратегија за хибридни закани не може целосно да биде имплементирана ако во неа не учествуваат сите актери во државата“, достапно на линк
- Министерство за одбрана (2020). Стратегија за сајбер-одбрана, достапно на: https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf

- Мицевски И., Трпевска С. (2024). Мониторинг на медиумскиот плурализам во дигиталната доба - Примена на мониторот на медиумскиот плурализам во земји членки на ЕУ и во земји-те-кандидатки во 2023 година - Национален извештај: Република Северна Македонија. Институт за истражување на општествениот развој – РЕСИС, достапно на: https://cadmus.eui.eu/bitstream/handle/1814/77022/North_Macedonia_MK_mpm_2024_cmpf.pdf?sequence=2&isAllowed=y

- Павловска Ј. (2024). Во спиралата на криминалот: Ред проневера, ред корупција и сè одново и повторно, Нова Македонија, достапно на: https://novamakedonija.com.mk/pecateno-izdanie/vo-spiralata-na-kriminalot-red-pronevera-red-korupcija-i-s%D1%90-odnovo-i-povtorno/

- Фајфер Х. (2024). Разоткриена мрежа за руска пропаганда во Европа, Дојче веле, достапно на: https://www.dw.com/mk/razotkriena-mreza-za-ruska-propaganda-vo-evropa/a-68698125

Институт за комуникациски студии

www.iks.edu.mk
info@iks.edu.mk

НЕ ВЕРУВАЈ ПРОВЕРУВАЈ! #користифакти

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

Овој производ е подготвен во рамките на проектот „Употреба на новинарство засновано на факти за подигање на свеста и спротивставување на дезинформациите во медиумскиот простор во Северна Македонија“, 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.

Институт за
комуникациски
студии

НЕ ВЕРУВАЈ
ПРОВЕРУВАЈ!
#користифакти