Институт за комуникациски студии

Насоки:
Одговор на владата на странското мешање и манипулирање со информации (СММИ) во Северна Македонија



Овие насоки ѝ обезбедуваат стратешка рамка на владата на Северна Македонија за справување со странското мешање и манипулирање со информации (СММИ). Главната цел е да се изгради општество што, долгорочно гледано, е поотпорно на дезинформации и истовремено да се заштити националната безбедност и слободата на говорот. Како гаранција дека оваа рамка ќе остане ефикасна, владата мора да се обврзе континуирано да ги истражува операциите на СММИ, користејќи ги лекциите научени од минатите мешања, за постојано усовршување и зајакнување на своите одбранбени мерки.

Дел 1: Зошто СММИ е национална закана

За да го заштити општеството, владата мора да го дефинира СММИ како закана за националната безбедност. За тоа да се направи ефективно, мора да се објаснат конкретните карактеристики на СММИ, врз основа на минати операции насочени кон Северна Македонија и кон поширокиот европски регион. Со анализа на овие повторувачки модели на дејствување, можеме да ја категоризираме опасноста низ четири различни призми: извор, начин, цел и влијание.

1. Извор

Суштински важно е да се направи разлика помеѓу домашните дезинформации и меѓународното мешање. Додека домашните дезинформации ги шират внатрешни актери како што се локални политичари или влијателни лица и тоа се прави за домашна корист, СММИ е управувано од актери поврзани со странска држава. СММИ обично тече низ комплексна мрежа дизајнирана да го скрие своето вистинско потекло.

- Официјални државни канали: Ова се официјални профили на странски влади, како што се дипломатски профили на социјалните медиуми, кои се користат за промовирање државни агенди.

- Медиуми под државна контрола: Наместо независни организации, овие функционираат како пропагандна машинерија - како што се RT и Sputnik - кои се финансирани од странски држави и немаат уредничка независност.

- Скриени усогласени канали: Ова вклучува прикриена мрежа или мрежа во сенка, составена од влијателни лица на социјалните медиуми, прокси односно посреднички веб-страници и автоматизирани бот-профили кои јавно не ги откриваат своите врски со странство, меѓутоа совршено ги отсликуваат државните наративи.

2. Начин

Одлики на СММИ се измамничко однесување и оперативни методи, а не само содржината на пораката. Овие дејства се специјално дизајнирани да ги измамат корисниците и да ја манипулираат техничката инфраструктура на дигиталните платформи.

- Дигитална мимикрија: Создавање „клонови“ на веб-страници што изгледаат идентично со кредибилни извори на вести, со цел да се измамат читателите, како што е операцијата Doppelgänger која ги имитираше големите европски медиуми, вклучувајќи ги *Le Parisien* и *Le Figaro* во Франција, *Der Spiegel* и *Bild* во Германија, *La Stampa* во Италија, *Gazeta Wyborcza* во Полска и *El Mundo* во Шпанија.

- Координирана неавтентична активност: Користење „фарми за ботови“ за истовремено објавување на истата порака за да се измамат алгоритмите за конкретна тема да стане тренд или да шират дезинформации. На пример: Истрагата на тимот Хорхе од истражниот колектив *Forbidden Stories* („Забранети приказни“) откри софтверски пакет што им овозможувал на операторите да контролираат над 30.000 софистицирани, верификувани профили на ботови на повеќе социјални платформи, за да манипулираат со јавното мислење и избори низ целиот свет.

- Хакирање и протекување: Крадење приватни информации и нивно стратешко објавување за да се наруши угледот на метата на нападот, метод што често се користи за нарушување на изборниот интегритет. На пример: за време на изборите во САД во 2016 година, украдени кампањски е-пораки беа протечени за да се манипулира јавното мислење.

- Deepfakes (Вештачки генерирана/манипулирана содржина): Користење вештачка интелигенција за креирање реалистична, но лажна видео или аудио содржина од лидери за да се предизвика забуна или паника. Светските лидери и политичките личности постојано се мета на вакви вештачки генерирани содржини во напади со дезинформации.

3. Цел

Целите на СММИ варираат во зависност од местото на актерот во мрежата, почнувајќи од државна стратегија на високо ниво до профит на ниско ниво.

- Политичка добивка: Странските влади имаат за цел да ги дестабилизираат ривалите или да влијаат врз важни одлуки. Операциите на СММИ го достигнуваат својот врв за време на некои клучни пресвртници. Во Северна Македонија: Во 2018 година, се користеа дезинформации за да се саботира Преспанскиот договор - договорот со кој се реши долгогодишниот спор за името со Грција за да се овозможи евроатлантска интеграција. Во Романија: За време на изборите во 2024 година, странското мешање користеше обемни координирани кампањи на социјалните медиуми за манипулирање со избирачкото тело.

- Финансиска добивка: Дезинформациите често се бизнис модел каде што „малите претприемачи“ се платени по клик. Случајот Велес: Тинејџери во Северна Македонија креирале содржина со која се поддржува Трамп пред изборите во САД во 2016 година, бидејќи сензационалистички лаги генерираат високи приходи од рекламирање.

4. Влијание

Надвор од директното политичко влијание, крајното влијание на СММИ е систематската ерозија на „социјалното лепило“ на земјата. Со преплавување на информациската средина со противречности, овие операции поттикнуваат длабока недоверба што ги наведува граѓаните да се сомневаат дури и во легитимните демократски институции. Понатаму, СММИ претставува директна закана за јавната безбедност; за време на кризи како пандемија или безбедносна вонредна состојба, странските дезинформации можат да ја доведат јавноста во заблуда во врска со безбедносните протоколи, што може да предизвика граѓански немири или јавно-здравствени катастрофи.

Дел 2: Како да се идентификува СММИ?

Идентификувањето на СММИ бара промена на фокусот. Наместо да се обидуваме да следиме или контролираме што велат луѓето, треба да ги анализираме специфичните тактики, техники и процедури (ТТП) што се користат за ширење на пораката. Со разложување на операцијата на овие три слоја, властите можат да препознаат странско мешање дури и кога самата содржина не е нелегална.

1. Тактики (стратегија)

Тактиките укажуваат на причините за операцијата. Тие се стратешките цели што странскиот актер сака да ги постигне, како што се „поделба на јавноста“ или „нарушување на довербата во институциите“.

- Пример: За време на преговорите за Преспанскиот договор, стратешката тактика била да се поткопа патот на Северна Македонија кон ЕУ и НАТО преку создавање длабоки поделби во општеството.

2. Техники (метод)

Техники се специфичните „трикови“ или методи што се користат за спроведување на тактика. Овој слој го опишува начинот на кој актерот го маскира својот идентитет или ја турка својата порака напред.

- Пример: Дигиталната мимикрија е честа техника каде што актерите создаваат лажни верзии на кредибилни веб-страници за да ја прикажат пропагандата како вистинска вест.

3. Процедури (извршување)

Процедурите се најдеталниот дел од анализата. Тие се технички постапки опишани чекор-по-чекор и специфични алатки што се користат за извршување на операцијата. Ова вклучува специфичен софтвер, време на објавување и потребни технички поставки.

- Пример: Користењето на софтверски пакет за управување со илјадници лажни профили одеднаш, како што може да се види во Истрагата на тимот Хорхе, е специфична постапка за „координирано неавтентично однесување“.

Со документирање на овие модели одн. обрасци, владата може да направи прирачник за мешање. Ова им овозможува на безбедносните агенции да идентификуваат напад врз основа на „црвени знамиња“ како предупредувачки знаци, давајќи им јасна причина да дејствуваат без да се мешаат во законското право на слобода на говор.

Дел 3: Како да се третира СММИ?

Успешниот одговор на СММИ не лежи само во разоткривањето на дезинформациите, бидејќи интеракцијата со странски лаги честопати дополнително ги шири лагите. Бидејќи корекциите како што е проверката на фактите не секогаш стигнуваат до сите или не го менуваат мислењето, владата мора да премине од реагирање кон проактивност. Ова значи градење „психолошка одбрана“ преку предвремено разоткривање, за да им помогне на граѓаните да ја забележат манипулацијата пред таа да пушти корен. Со вклучување на целото општество, државата може да ја заштити информациската средина без прибегнување кон цензура. На крајот на краиштата, овој пристап ја зајакнува националната безбедност, воедно грижејќи се за безбедноста на демократските вредности.

1. Предвремено разоткривање (Prebunking)

Иако разоткривањето (коригирање лага откако ќе се прошири) е неопходна реактивна алатка, таа често не е толку ефикасна бидејќи првобитната лага веќе се вкоренила во умот на јавноста. Предвременото разоткривање вклучува учење на граѓаните да ги препознаваат триковите на манипулација - како што се предизвикувачите на емоционални реакции или употребата на лажни експерти - пред да се сретнат со дезинформацијата. Со информирање на јавноста за методите што се користат во СММИ, владата гради долгорочна отпорност за општеството, правејќи ги дезинформациите помалку влијателни кога се појавуваат. Ова може да се постигне на повеќе начини.

- Учење преку игра: Интерактивни алатки, како играта „Лоши вести“ им овозможуваат на корисниците да глумат лоши актери. Со користење тактики на манипулација за добивање лажни следбеници, играчите учат да ги забележуваат истите тие црвени знамиња во објавите што им се појавуваат на социјалните мрежи.

- Разјаснувачки видеа: кратки, неутрални видеа што објаснуваат вообичаени трикови за манипулација, а не конкретни приказни. На пример: видеото може да објасни што е „жртвено јагне“, така што кога некој ќе види напад со тој трик, веднаш ќе ја препознае техниката.

2. Принципот „Не прави штета“

Секоја владина акција мора внимателно да се избалансира за да се заштити националната безбедност без да се наруши слободата на говорот.

- Да се избегне прекумерна регулација: строгите закони честопати предизвикуваат „ефект на одвраќање“ каде што платформите прекумерно бришат содржина за да избегнат високи казни, што ја задушува здравата јавна дебата. За да се спречи ова, владите не треба да забрануваат содржина, туку да бараат поголема транспарентност, како што се јавни репозитари за рекламирање што откриваат кој платил за манипулативни реклами. Овој пристап ги охрабрува платформите да користат етикети и предупредувања - слични на банерите за проверка на факти на Мета - за да ги информираат корисниците за потенцијални дезинформации без да ги замолчуваат или да ги отстрануваат нивните објави.

- Да се таргетира прашањето „Како“, а не „Што“: владата треба да се фокусира на запирање на „машинеријата“ зад лагите. Ова значи таргетирање на „фармите за

ботови“ и лажните профили, а не на индивидуалните мислења, бидејќи е многу побезбедно за демократијата да избрише 10.000 компјутерски управувани профили отколку да цензурира еден вистински граѓанин. Со користење на закони како што е Законот за дигитални услуги (DSA), државата може да изврши притисок врз компаниите на социјалните медиуми да ги обезбедат своите платформи за да не можат повеќе да бидат експлоатирани од странски актери.

- Независност: за да се осигури дека напорите против дезинформациите никогаш нема да се злоупотребат за политичка корист, надзорот мора да го вршат независни агенции. Ова вклучува мрежи за проверка на факти, веродостојни медиуми, како и невладини организации (како што е Alliance4Europe) кои дејствуваат како чувари за заштита на дигиталните права. Со овластување на независни експерти наместо политичари, државата гарантира дека активностите се насочени само кон реални странски закани. Со тоа се спречува злоупотреба на алатките против дезинформации за политичка добивка.

3. Пристапот на општеството како целина

СММИ е комплексна закана што не може да се реши од едно министерство; таа бара координирана национална стратегија. Владата треба да воспостави обединето тело кое ќе ги вклучува надворешните работи, одбраната, внатрешните работи и образованието за споделување разузнавачки информации и планирање одговори. Со транспарентна комуникација со независните медиуми и невладините организации, државата ја зајакнува медиумската писменост и гради поинформирана јавност без мешање на владата.

Градењето отпорно општество бара посветеност на образованието на секое ниво. Министерството за образование мора да ја интегрира медиумската писменост во училиштата, фокусирајќи се на тоа како функционираат демократските системи и како наративите се користат за манипулирање со историјата или науката. Министерството за информатичко општество треба да се фокусира на дигиталните вештини, помагајќи им на граѓаните да разберат како функционираат алгоритмите на платформите и како да идентификуваат „вирални“ трендови предводени од ботови.

4. Меѓународна соработка

СММИ е прекугранична закана за која треба мрежа што ќе се бори против друга мрежа. Со синхронизирање со европските рамки, Северна Македонија може да има пристап до напредни алатки и да биде сигурна дека нејзината медиумска средина ги исполнува меѓународните демократски стандарди.

- Комплетот со алатки за СММИ: Владата треба да го усвои комплетот со алатки за СММИ на ЕУ, кој вклучува следење, откривање, системи за брзо предупредување и дипломатски одговори како што се санкции врз медиуми спонзорирани од странски држави.

- Зајакнување на саморегулацијата: Поттикнување на медиумите да ги следат професионалните етички кодекси, па дури и да аплицираат за соработка и членство во Европската мрежа за стандарди за проверка на факти (EFCSN) или глобалната Меѓународна мрежа за проверка на факти (IFCN).

Со усвојување на овој проактивен и инклузивен модел, Северна Македонија може да ја брани својата национална безбедност, а воедно да ги зајакне - наместо да ги ослабне - демократските права на своите граѓани.

Институт за комуникациски студии



British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

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