NDËRHYRJET E HUAJA DHE MANIPULIMI ME INFORMACIONET NË REPUBLIKËN E MAQEDONISË SË VERIUT

Analizë fillestare

NDËRHYRJET E HUAJA DHE MANIPULIMI ME INFORMACIONET NË REPUBLIKËN E MAQEDONISË SË VERIUT

Analizë fillestare

Botues:
Instituti për Studime të Komunikimit
rr. „Jurij Gagarin“ 17-1 / 1, Shkup
www.iks.edu.mk

Rreth botuesit:
prof. dr. ZanetaTrajkoska

Edicioni:
ResPublica

Autore:
prof. ordiner Metodi Haxhi-Janev
dr. Marijan Stoillkovski

Redaktor:
mr. Dejan Andonov

Përkthyer nga gjuha maqedonase:
Vjosa Taipi

Titulli origjinal:
Странско мешање и манипулирање со информации - појдовна анализа

Dizajn grafik:
Igor Delov

Vendi dhe viti:
Shkup, 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)

HAXHI-Janev, Metodi
Ndërhyrjet e huaja dhe manipulimi me informacionet në Republikën e Maqedonisë së Veriut [Електронски извор] : analizë fillestare / [autore Metodi Haxhi-Janev, Marijan Stoillkovski ; përkthyer nga gjuha maqedonase Vjosa Taipi]. - Shkup : Instituti për Studime të Komunikimit, 2025. - (Edicioni ResPublica)

Начин на пристапување (URL):
http://respublica.edu.mk/wp-content/uploads/2025/05/nderhyrjet-e-huaja-dhe-manipulimi-me-informacionet-rsm.pdf.
- Превод на делото: Странско мешање и манипулирање со информации : појдовна анализа. - Текст во PDF формат, содржи 70 стр. - Наслов преземен од екранот. - Опис на изворот на ден 02.06.2025. - Фусноти кон текстот. - Rreth autorëve: стр. 65. - Библиографија: стр. 66-70

ISBN 978-608-4805-62-5

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

COBISS.MK-ID 66063109

PËRMBAJTJA

	Rezyme	6
	Hyrje	7
	Metodologjia	9
1.	**Ndërhyrjet e huaja dhe manipulimi me informacionet: nocioni dhe karakteristikat**	11
1.1.	Përcaktimi i ndërhyrjes së huaj dhe manipulimi me informacionet	13
1.2.	Si manifestohet ndërhyrja e huaj dhe manipulimi me informacionet	14
2.	**Kapacitetet institucionale dhe dobësitë në Maqedoninë e Veriut gjatë përballjes me ndërhyrjet e huaja dhe manipulimin me informacionet**	17
2.1.	Shqyrtimi i përgjithshëm i kapaciteteve institucionale në Maqedoninë e Veriut për përballje me ndërhyrjen e huaj dhe manipulimin me informacionet	19
2.2.	Kuadri ligjor dhe rregullator	20
2.3.	Shqyrtim kritik: Sfidat institucionale në Maqedoninë e Veriut për përballje me ndërhyrjen e huaj dhe manipulimin me informacionet	23
2.3.1.	Shqyrtimi i kapacitetit shtetëror për t'iu përgjigjur fushatave të dezinformimit	28
2.4.	Analiza dhe shqyrtimi kritik i rolit të komunitetit lokal si objektiv i ndërhyrjes së huaj dhe manipulimit me informacionet	31
3.	**Roli i mediave dhe sektorit civil në Maqedoninë e Veriut dhe cenueshmëria ndaj ndërhyrjeve të huaja dhe manipulimit me informacionet**	33
3.1.	Roli i medias në trajtimin e ndërhyrjeve të huaja dhe manipulimin me informacionet	34
3.2.	Roli i shoqërisë civile në trajtimin e ndërhyrjeve të huaja dhe manipulimin me informacionet	36

4.	**Krimi kibernetik dhe rrjetet sociale si mjete për ndërhyrjet e huaja dhe manipulimin me informacionet**	40
4.1.	Lidhja e ndërsjellë e sulmeve kibernetike dhe dezinformatat për manipulim	42
4.2.	Krimi kibernetik dhe dezinformatat si rrezik për sektorin ekonomik	45
4.3.	Mekanizma për siguri kibernetike dhe mbrojtje nga dezinformatat	47
4.4.	Këshilla për mbrojtje nga kërcënimet kibernetike	48
5.	**Përmbledhje e shkurtër e praktikave të mira evropiane në trajtimin e ndërhyrjeve të huaja dhe manipulimit me informacionet**	51
5.1.	Praktikat e suksesshme në disa vende të BE-së	53
5.1.1.	Forcimi i reagimit institucional: modele të suksesshme	53
5.1.2.	Kuadri rregullator: si mund ta mbrojë ligji demokracinë?	54
5.1.3.	Ndërgjegjësimi i publikut dhe edukimi mediatik: një linjë kyçe e mbrojtjes	55
5.2.	Përmbledhje e praktikave dhe përvojave të mira të BE-së dhe NATO-s në përballjen me ndërhyrjen e huaj dhe manipulimin me informacionet	56
5.2.1.	Task Forca për Komunikim Strategjik - Lindje e BE-së (East StratCom Task Force)	57
5.2.2.	Qendra e Ekselencës për Kërcënimet Hibride (Hybrid Center of Excellence): mbrojtja hibride përmes analizës dhe koordinimit strategjik	58
5.2.3.	Sistemi për Alarmim të Shpejtë e BE-së (Rapid Alert System): përgjigje e shpejtë ndaj kërcënimeve informative	59
	Rekomandime për krijimin e politikave për trajtimin e ndërhyrjeve të huaja dhe manipulimin me informacionet në Maqedoninë e Veriut	60
	Përfundim	63
	Rreth autorëve	65
	Literatura e përdorur	66

REZYME

Ky studim hulumton mekanizmat, metodat dhe efektet e ndërhyrjes së huaj dhe manipulimit me informacionet (NHMI) në Republikën e Maqedonisë së Veriut, me theks të veçantë në sigurinë kombëtare, koloritin mediatik dhe kohezionin social. Si një vend me pozitë strategjike në rajon, anëtar i NATO-s dhe kandidat për Bashkimin Evropian (BE), Maqedonia e Veriut përballet me kërcënime informative të shtuara që vijnë nga aktorë të ndryshëm shtetërorë dhe jo-shtetërorë. Këto ndikime kanë potencialin të prishin proceset demokratike, të dobësojnë institucionet dhe të nxisin mosbesimin e publikut.

Studimi tregon se ndërhyrja e huaj dhe manipulimi me informacionet nuk është një fenomen i izoluar, por pjesë e strategjive më të gjera hibride që kombinojnë dezinformimin, narrativat gjeopolitike dhe operacionet kibernetike për të formuar opinionin publik dhe vendimet politike. Analiza mbulon disa fusha, duke përfshirë gatishmërinë institucionale (referuar qeverisjes së mirë), mediat tradicionale, hapësirën digjitale dhe rrjetet sociale, komunitetet lokale dhe organizatat e shoqërisë civile, duke identifikuar metodat dhe qasjet kryesore të përdorura për polarizimin politik dhe ideologjik.

Pavarësisht ekzistencës së kornizave ligjore dhe institucionale për përballje me ndërhyrjen e huaj dhe manipulimin me informacionet, kapaciteti kombëtar për detektimin dhe kundërveprimin mbetet i kufizuar dhe i paqëndrueshëm. Analiza tregon se është e nevojshme një qasje më gjithëpërfshirëse, e cila do të përfshijë koordinim më të mirë midis institucioneve shtetërore, sektorit civil dhe komunitetit mediatik. Është veçanërisht e rëndësishme të promovohet qeverisja e mirë e organeve shtetërore, të rriten mekanizmat rregullatorë për transparencë në media, të forcohen kapacitetet analitike për të monitoruar kërcënimet digjitale dhe për të ndërtuar qëndrueshmëri në mesin e publikut përmes edukimit mediatik.

Ky studim ofron rekomandime për përmirësimin e strategjive për trajtimin e ndërhyrjeve të huaja dhe manipulimin me informacionet, me fokus në masat parandaluese dhe reaktive që do të mundësojnë mbrojtjen e hapësirës informative në Maqedoninë e Veriut. Rekomandimet përfshijnë reforma strukturore, përmirësimin e bashkëpunimit ndërkombëtar dhe zhvillimin e mekanizmave kombëtarë për zbulimin dhe neutralizimin e fushatave të dezinformimit. Roli i institucioneve shtetërore, medias dhe shoqërisë civile është thelbësor në këtë luftë, sepse vetëm përmes një qasjeje të përbashkët mund të minimizohen pasojat e ndikimeve informative të huaja dhe të mbrohen vlerat demokratike dhe interesat e sigurisë së vendit.

HYRJE

Në botën e sotme të globalizuar, informacioni paraqet një mjet të fuqishëm që mund të përdoret si një instrument për të ndikuar në shoqëri, procese politike dhe politika të sigurisë. Ndërhyrja e huaj dhe manipulimi me informacionet përbën një sfidë serioze për sigurinë kombëtare, besimin publik dhe institucionet demokratike. NHMI-ja përfshin një gamë të gjerë aktivitete, duke përfshirë dezinformimin, sulmet kibernetike, propagandën mediatike dhe fushatat e koordinuara me ndikim që synojnë të minojnë proceset demokratike, të shkaktojnë ndarje në shoqëri dhe të dobësojnë institucionet shtetërore.

Në kontekstin e Maqedonisë së Veriut, e cila është shtet anëtar i NATO-s dhe kandidat për anëtarësim në BE, ky kërcënim merr një rëndësi të veçantë. Si një vend i pozicionuar në mënyrë strategjike në Ballkan, Maqedonia e Veriut është e ekspozuar ndaj formave të ndryshme të ndikimit të huaj që shpesh përfshijnë manipulimin me informacione në mënyrë që të minojnë besimin e publikut në institucione, të gjenerojnë paqëndrueshmëri politike ose të pengojnë integrimin euro-atlantik. Aktorët e jashtëm, duke përdorur mjete të përparuara digjitale, rrjetet sociale dhe mediat tradicionale, po kryejnë gjithnjë e më shumë operacione informacioni që synojnë sektorët kryesorë në vend.

Ky studim fillestar synon të përcaktojë natyrën, qëllimin dhe metodat e ndërhyrjes së huaj dhe manipulimit të informacionit në Maqedoninë e Veriut. Për më tepër, do të analizohen dobësitë, rreziqet dhe ndikimet në institucionet publike, mediat dhe shoqërinë civile në mënyrë që të përcaktohet niveli i ekspozimit të Maqedonisë së Veriut ndaj kërcënimeve të NHMI-së.

Për të pasur një pasqyrë të detajuar të cenueshmërisë ndaj ndërhyrjes së huaj dhe manipulimit të informacionit dhe efekteve që mund të shkaktohen nga një veprim i tillë, analiza do të përqendrohet në disa aspekte kryesore. Së pari, do të flasim për mënyrën se si institucionet publike merren me NHMI-në, dhe lidhur me atë nëse ka dobësi strukturore apo njerëzore. Në këtë seksion do të diskutohet korniza ligjore dhe rregullatore, kapacitetet institucionale dhe qasja dhe aftësia për t'iu përgjigjur fushatave për dezinformata. Më pas, analiza do të përqendrohet në mediat dhe rrjetet sociale, si dhe në atë se cili është roli i komunitetit lokal (duket një segment subversiv) si një objektiv ndikimi dhe në trajtimin e këtyre sfidave. Analiza përqendrohet gjithashtu në shkrirjen e krimit kibernetik dhe dezinformatave, veçanërisht përmes rrjeteve sociale.

Përmes hartëzimit të politikave dhe kornizave ekzistuese të NATO-s dhe BE-së, si dhe mekanizmat në dispozicion të institucioneve kombëtare, studimi do të identifikojë kapacitetet kryesore për të luftuar ndërhyrjen e huaj dhe manipulimin me informacionet. Bazuar në këtë analizë, do të propozohen praktikat dhe rekomandimet më të mira për të forcuar qëndrueshmërinë në sferat sociale, mediatike dhe kibernetike, me qëllimin përfundimtar të forcimit të sigurisë kombëtare dhe stabilitetit demokratik të Maqedonisë së Veriut.

METODOLOGJIA

Ky studim bazohet në desktop analizën si një qasje metodologjike kryesore për të eksploruar fenomenin e ndërhyrjes së huaj dhe manipulimit të informacionit në Maqedoninë e Veriut. Kjo qasje nënkupton mbledhjen, përpunimin dhe sintezën e informacionit tashmë ekzistues nga burimet përkatëse në mënyrë që të kemi një pasqyrë gjithëpërfshirëse për natyrën, metodat dhe ndikimin e NHMI-së, në sigurinë kombëtare dhe stabilitetin shoqëror. Këto të dhëna u përpunuan më pas falë përvojës profesionale dhe akademike të autorëve.

Hulumtimi bazohet në analizën e dokumenteve zyrtare, raporteve dhe kornizave rregullatore, të cilat përfshijnë strategjitë qeveritare për ballafaqim me kërcënimet hibride, sigurinë kibernetike, edukimin mediatik dhe sigurinë kombëtare. Për më tepër, analiza mbulon dokumente nga institucionet përkatëse të sigurisë në Maqedoninë e Veriut, NATO dhe BE, si dhe rregulloret ligjore në lidhje me luftimin e dezinformatave dhe ndikimin e huaj. Për një kuptim më të thellë të problemit, studimi përfshin hulumtimin e kryer nga grupet e ekspertëve ndërkombëtarë, qendrat kërkimore dhe organizatat që punojnë në çështjet që lidhen me kërcënimet hibride dhe dezinformatat, siç janë Qendra e Ekselencës StratCom e NATO-s (NATO StratCom Center of Excellence), Qendra Hibride e Ekselencës e BE-së dhe NATO-s për Luftë Kundër Kërcënimeve Hibride (Hybrid Center of Excellence) dhe Task Forca për komunikime strategjike - Lindje e BE-së (East StratCom Task Force), duke përfshirë, jo më pak e rëndësishme, përvojën e autorëve në bashkëpunimin me këto institucione për temën dhe problemin në fjalë.

Përveç burimeve akademike dhe institucionale, analiza mbulon publikime mediatike dhe raporte të OJQ-ve që merren me transparencën mediatike dhe monitorimin e hapësirës informative. Theks i veçantë i kushtohet rolit që luajnë mediat dhe platformat sociale në përhapjen e dezinformatave.

Metodologjikisht, studimi zbaton analizën cilësore të përmbajtjes për të identifikuar narrativet kryesore, metodat dhe aktorët e përfshirë në ndërhyrjen e huaj dhe manipulimin me informacionet. Kjo qasje lejon kategorizimin sistematik të teknikave të përdorura në operacionet informative, duke përfshirë dezinformimin, manipulimin e mediave, trillimin e lajmeve, sulmet kibernetike dhe strategjitë e propagandës gjeopolitike. Për më tepër, analiza krahasuese përdoret për të krahasuar kontekstin maqedonas me përvoja të ngjashme nga vendet e tjera të rajonit, gjë që lejon një kuptim më të mirë të modeleve dhe dinamikës së kërcënimeve të NHMI-së.

Për më tepër, hulumtimi analizon faktorët që rrisin cenueshmërinë e Maqedonisë së Veriut ndaj ndërhyrjes së huaj dhe manipulimit të informacioneve, siç janë dobësitë në edukimin mediatik, kapacitetet institucionale dhe polarizimin politik. Analiza politike dhe normative, nga ana tjetër, lejon vlerësimin e mekanizmave ekzistues për trajtimin e këtyre kërcënimeve, si dhe efektivitetin e tyre në lidhje me interesat kombëtare dhe prioritetet e sigurisë së vendit.

Ndërsa ky hulumtim ofron analizë të thellë të ndërhyrjes së huaj dhe manipulimit me informacionet në Maqedoninë e Veriut, duhet të merren parasysh disa kufizime. Mungesa e të dhënave transparente, konfidencialiteti i informacioneve të inteligjencës dhe natyra dinamike e fushatave dezinformuese paraqesin sfidë për një vlerësim të plotë dhe objektiv të problemit. Përkundër këtyre kufizimeve, ky studim synon të ofrojë një pasqyrë sistematike të natyrës, metodave dhe ndikimit të NHMI-së në vend. Bazuar në këto gjetje, studimi propozon rekomandime për forcimin e qëndrueshmërisë kombëtare në sferat sociale, mediatike dhe kibernetike, me qëllimin përfundimtar të forcimit të sigurisë dhe stabilitetit demokratik të Maqedonisë së Veriut.

1.

NDËRHYRJET E HUAJA DHE MANIPULIMI ME INFORMACIONET: NOCIONI DHE KARAKTERISTIKAT

Në hapësirën moderne globale informative, ndërhyrja e huaj dhe manipulimi me informacionet paraqet një nga kërcënimet më të sofistikuara dhe destruktive për proceset demokratike, sigurinë kombëtare dhe kohezionin social. Ky fenomen bazohet në përdorimin strategjik dhe të qëllimshëm të informacioneve me qëllim të ndikohet në vendimet e qytetarëve, institucioneve dhe qeverive, kryesisht në dobi të aktorëve të huaj.

Ndërhyrja e huaj dhe manipulimi me informacionet nuk është vetëm dezinformim klasik. Është një mekanizëm kompleks që kombinon taktikat e propagandës, manipulimin e mediave, destabilizimin përmes rrjeteve sociale, presionet ekonomike dhe politike, madje edhe aktivitetet kibernetike. Thelbi i tyre qëndron në shtrembërimin e kontrolluar të peizazhit informativ për të arritur ndikim gjeopolitik afatgjatë.

1.1. PËRCAKTIMI I NDËRHYRJES SË HUAJ DHE MANIPULIMI ME INFORMACIONET

E thënë thjesht, ndërhyrja e huaj dhe manipulimi me informacionet paraqet një aktivitet të organizuar, të qëllimshëm dhe shpesh aktivitet i fshehtë i aktorëve shtetërorë ose jo-shtetërorë që synojnë manipulimin e mjedisit informativ, për të arritur një avantazh politik, ushtarak, ekonomik ose social *(EEA, 2023)*. Karakteristikat kryesore të NHMI-së përfshijnë *(Diplomatic Service of EU, 2025):*

- **qasje manipuluese** – përmes informacioneve të fabrikuara, të manipuluara ose të paraqitura në mënyrë selektive për të krijuar një pamje të rreme të realitetit;

- **aktivitete të tilla kanë një qëllim strategjik** – qëllimi nuk është vetëm dezinformimi, por edhe ndikimi në publik, në institucione ose ndikim mbi vendimmarrësit dhe në këtë mënyrë të korruptohen proceset demokratike;

- **zbatimi i taktikave dhe kanaleve të ndryshme** – përdorimi i NHMI-së nënkupton kombinimin e metodave të propagandës klasike, manipulimeve digjitale, sulmeve kibernetike, madje edhe instrumenteve ekonomike dhe diplomatike (për shembull, përmes diplomacisë shumë-shtresore ose "Multitrack Diplomacy", përkatësisht diplomacisë përgjatë pistës dytësore "Track -II Diplomacy ") *(Diamond L., McDonald J., 1996)*.

- **komplekse për të zbuluar dhe gjurmuar** – ndryshe nga dezinformimi konvencional, NHMI-ja shpesh kryhet në nivele të shumëfishta, me narrativë komplekse dhe rrjete të koordinuara aktorësh, shpesh të fshehura me mjeshtëri midis proceseve legjitime demokratike.

Ndërhyrja e huaj dhe manipulimi me informacionet është projektuar për të vepruar në mënyrë shumëdimensionale. Sulmojnë institucionet, por jo drejtpërdrejt, por përmes qasjes tek qytetarët, falë keqpërdorimit të teknologjive moderne informative dhe komunikuese, ndërsa së fundmi përmes të ashtuquajturave teknologji transformuese ose shqetësuese që janë në rritje. Kjo u lejon të ndikojnë përmes kontrollit ose vendosjes së kontrollit mbi përmbajtjen me të cilën (dez)informojnë qytetarët, mbledhjen e të dhënave dhe përpunimin e atyre të dhënave përmes sulmeve kibernetike, manipulimit të motorëve të kërkimit në internet dhe algoritmeve për

shpërndarje dhe kërkim, etj. Prandaj, NHMI nuk është vetëm një kërcënim për përdoruesit individual të informacioneve, por edhe një kërcënim për institucionet duke krijuar kaos informativ, ndarje sociale dhe politike.

1.2. SI MANIFESTOHET NDËRHYRJA E HUAJ DHE MANIPULIMI ME INFORMACIONET

NHMI nuk kufizohet vetëm në një formë të manipulimit. Përkundrazi, ajo manifestohet përmes taktikave të ndryshme, të cilat përshtaten me vendin e synuar dhe kontekstin specifik. Format më të zakonshme të ndërhyrjes së huaj dhe manipulimit me informacionet përfshijnë: dezinformimin dhe propagandën, keqpërdorimin dhe manipulimin e hapësirës mediatike dhe rrjeteve sociale, sulmet kibernetike edhe përmes mjeteve të dizajnuara posaçërisht për këtë, ndikimin dhe manipulimin përmes sektorëve ekonomikë dhe diplomatikë për të amplifikuar kaosin e përgjithshëm në një qasje të kombinuar me procedurat e mëparshme.

Ndërhyrja e huaj dhe manipulimi me informacionet përfshin metodat e avancuara të propagandës klasike dhe shpërndarjen e dezinformatave dhe propagandës. Këto përfshijnë shpërndarjen e qëllimshme të informacioneve të rreme, të shtrembëruara ose të manipuluara për të minuar besueshmërinë e institucioneve, mediave ose individëve *(Boulianne Sh., Humprecht E, 2023)*. NHMI-ja gjithashtu përfshin krijimin e narrativave të rreme për të diskreditуar kundërshtarët politikë ose për të forcuar një agjendë të veçantë, zakonisht duke përdorur tensionet historike, etnike dhe fetare për të krijuar ndarje në shoqëri *(Miguel R., 2024)*.

Manipulimi i mediave dhe rrjeteve sociale është gjithashtu një teknikë e zakonshme në zbatimin e këtyre praktikave *(Kelly S. at all, 2017)*. Shpesh përfshin kontrollin ose infiltrimin në mediat lokale, përmes formave të ndryshme, donacioneve, sponsorizimeve të projekteve ose pronësisë së plotë dhe instalimit të bordeve editoriale të prira drejt përhapjes së informacionit të rremë dhe manipulimin e informacionit që synon të formësojë diskursin publik. Manipulimi i hapësirës mediatike përfshin gjithashtu praktikën e krijimit të platformave të mediave të rreme që imitojnë burimet përkatëse,

por shpërndajnë përmbajtje propagandistike *(CISA, 2023)*. Përdorimi i boteve, trolleve dhe fushatave të koordinuara për shpërndarjen masive të përmbajtjes manipuluese janë një shumëzues shtesë në manipulime *(Walker Sh., Simeone M., 2020)*.

Sulmet kibernetike janë pjesë integrale e ndërhyrjes së huaj dhe strategjive të manipulimit me informacionet. Këto përfshijnë:

- **hakerimi dhe nxjerrja e të dhënave të ndjeshme** duke përfshirë sulmet për të kompromentuar figurat politike ose institucionet;

- **kryerjen e sulmeve përmes mohimit të shpërndarjes së shërbimeve (Distributed Denial of Services DDoS)** në portalet e mediave ose në faqet e internetit të qeverisë për të zvogëluar disponueshmërinë e tyre;

- **raporte të rreme ose informacione** që shkaktojnë panik për të paralizuar ose testuar, përkatësisht për të zhvendosur sistemin dhe për të krijuar një intolerancë kumulative ndaj qeverisë/udhëheqjes;

- **manipulimi i algoritmeve të rrjeteve sociale** për promovimin ose kufizimin e narrativa të caktuara (për të ridrejtuar trafikun, për të bllokuar, për të zvogëluar ose për të shpejtuar mbingarkesën).

Megjithëse adresohet pak në Maqedoninë e Veriut, ndërhyrja e huaj dhe manipulimi me informacionet shpesh përkthehen përmes kanaleve ekonomike dhe diplomatike. Përveç kësaj, kjo mund të përfshijë:

- **shfrytëzimin e investimeve strategjike, ndihmës ekonomike, kredive dhe përdorimin e lirisë së tregut** për të fituar ndikim mbi mediat, institucionet akademike ose elitat politike, përmes vendeve të treta (zakonisht partnere);

- **përdorimi i varësisë energjetike ose lidhjeve tregtare** për të imponuar një agjendë politike;

- **presioni diplomatik** përmes mediave propagandistike të financuara nga qeveritë e huaja (për shembull, „Rusia sot“ (Russia Today), „Sputnik“ dhe të tjerë).

Përdorimi i një fushate të sinkronizuar tregon se NHMI nuk ndodh në mënyrë sporadike (edhe pse intensiteti mund të ndryshojë) dhe nuk zbatohet rastësisht. Përkundrazi, pas të gjitha veprimeve qëndrojnë objektivat strategjikë që shpesh synojnë (EUEA, 2023):

- **delegjitimimin e demokracisë dhe institucioneve** – minimin e besimit të qytetarëve në qeveritë e tyre dhe krijimin e një perceptimi të joefikasitetit dhe korrupsionit;
- **polarizimi politik** – nxitja e konflikteve midis grupeve të ndryshme në shoqëri me qëllim dobësimin e kohezionit social;
- **manipulimi i proceseve zgjedhore** – ndikimi në opinionin publik përmes fushatave dezinformuese, veçanërisht gjatë zgjedhjeve;
- **minimi i aleancave të sigurisë (NATO, BE)** – krijimi i një perceptimi se institucionet perëndimore janë të dobëta, të ndara ose të paafta për të siguruar stabilitet.
- **forcimi i ndikimit të shteteve autoritare** – promovimi i narrativave që paraqesin modelin autoritar si më efektiv dhe të dëshirueshëm sesa demokracia liberale *(EUEA, 2025)*.

Megjithatë edhe pse NHMI nuk është një fenomen i thjeshtë, ndikimi i tij mund të reduktohet ndjeshëm nëpërmjet një qasjeje strategjike dhe gatishmërisë së fortë institucionale.

2.

KAPACITETET INSTITUCIONALE DHE DOBËSITË NË MAQEDONINË E VERIUT GJATË PËRBALLJES ME NDËRHYRJET E HUAJA DHE MANIPULIMIN ME INFORMACIONET

Manipulimi me informacionet nga shërbimet e huaja në mënyrë të drejtpërdrejtë ose përmes proksi aktorëve paraqet një sfidë serioze për institucionet në Maqedoninë e Veriut. Në kushtet e konkurrencës dhe digjitalizimit të intensifikuar gjeopolitike. Kapaciteti i fortë institucional për përballje me NHMI-në është vërtet i nevojshëm. Prandaj, nevojitet një kuptim i dobësive dhe mangësive institucionale për të zhvilluar rekomandime.

2.1. SHQYRTIMI I PËRGJITHSHËM I KAPACITETEVE INSTITUCIONALE NË MAQEDONINË E VERIUT PËR PËRBALLJE ME NDËRHYRJEN E HUAJ DHE MANIPULIMIN ME INFORMACIONET

Kjo është analiza e parë e gatishmërisë së institucioneve në Maqedoninë e Veriut për pallafaqim me NHMI-në. Ajo fokusohet në kuadrin ligjor dhe rregullator ekzistues, kapacitetin institucional (agjencitë qeveritare dhe qasja e tyre – reaktive/proaktive), koordinimin dhe komunikimin ndërinstitucional dhe qasjen ndaj fushatave për dezinformata.

Konstatimet, me pak fjalë, janë se institucionet maqedonase janë ende në një fazë të hershme për sa i përket kuptimit të plotë dhe trajtimit efektiv me NHMI-në. Ndërgjegjësimi i përfaqësuesve politikë për kërcënimin nga NHMI është vetëm deklarativ. Përfaqësuesit institucionalë e njohin kërcënimin, shpesh si pjesë e kërcënimeve hibride. Fatkeqësisht, në praktikë, ka shumë pak gjëra që mund të përdoren për të matur realisht nëse ndërgjegjësimi i kërcënimit është në nivelin e duhur (EU Commission, 2023). Për shembull, ndërsa në fjalimet e tyre në ngjarje publike, përfaqësuesit politikë e njohin me të drejtë kërcënimin (MPB, 2022), në praktikë mund të shihen shumë pak veprime për ta kundërshtuar atë. Për shembull, nuk ka të dhëna për fonde nga buxheti i shtetit për ngritjen e kapaciteteve për të adresuar këtë sfidë. Në vend të kësaj, të gjitha aktivitetet e trajnimit dhe ngritjes së kapaciteteve kryhen me financim nga donatorët.

Strategjia për Kundër Kërcënimeve Hibride është dokumenti i vetëm që trajton me kujdes problemin e ndërhyrjeve të huaja dhe manipulimit të informacionit (Qeveria e Republikës së Maqedonisë, 2021). Dokumenti është i disponueshëm në faqen e internetit të Ministrisë së Mbrojtjes, e cila udhëhoqi zhvillimin e strategjisë. Përderisa Qeveria ka ngarkuar Këshillin Koordinues të Komunitetit të Sigurisë dhe Inteligjencës që të delegojë zbatimin e detyrave të Strategjisë dhe Planit të Veprimit, në praktikë ky Këshill nuk është funksional.

Ekzistenca e Strategjisë është një fillim i mirë, por duhet bërë më shumë për ta funksionalizuar atë.

2.2. KUADRI LIGJOR DHE RREGULLATOR

Në Maqedoninë e Veriut, në legjislacion mungojnë masa të specializuara për ndërhyrjen e huaj dhe manipulimin me informacionet.. Megjithëse ekzistojnë disa dispozita që synojnë tema që lidhen me ndërhyrjen e huaj dhe manipulimin me informacionet në disa nga zgjidhjet ligjore, siç janë Kodi penal dhe Ligji për mbrojtjen e të dhënave personale ose Ligji për ndryshime dhe plotësime të Ligjit për mbrojtjen e të dhënave personale, është e qartë se vetëm këto dispozita nuk janë të mjaftueshme për ballafaqim të drejtpërdrejtë me NHMI-në. Mungesa e ligjeve ose akteve nënligjore të veçanta që synojnë drejtpërdrejt ndikimin e huaj në hapësirën informative vetëm konfirmon se kuadri ligjor dhe rregullator në vend për përballje me NHMI-në nuk është zhvilluar sa duhet.

Zgjidhjet përkatëse ligjore, nga ku duhet të nxirret baza për qasje në trajtimin e ndërhyrjeve të huaja dhe manipulimin me informacione, përfshijnë Ligjin për Procedurën Penale, Kodin Penal, Ligjin për përgjimin e komunikimeve dhe Ligjin për komunikimet elektronike, të cilat, ndër të tjera, rregullojnë sigurinë e të dhënave personale dhe përcaktojnë shprehjet që kanë një rol të rëndësishëm në komunikimin përmes hapësirës në internet të qytetarëve të Maqedonisë. Për më tepër, zgjidhjet ligjore që duhet të merren parasysh janë: Ligji për mediat, Ligji për shërbimet mediatike audio dhe audiovizive, Ligji për parandalimin e pastrimit të parave dhe financimit të terrorizmit, Ligji për përgjegjësinë civile për fyerje dhe shpifje[1], Ligji për mbrojtjen e fëmijëve (i cili rregullon sistemin dhe organizatën për mbrojtjen e fëmijëve) dhe Ligji për drejtësinë e fëmijëve. Duke pasur parasysh kompleksitetin e ndërhyrjes së huaj dhe manipulimin me informacionet, mund të thuhet se kjo listë e zgjidhjeve ligjore nuk përfundon këtu. Për shembull, përveç dezinformatave dhe propagandës, fushëveprimi i NHMI-së përfshin operacionet për ndikimin përmes sulmeve kibernetike, në mënyrë që ose të ndryshohen informacionet zyrtare dhe të krijohet pasiguri dhe dezinformim ose të eksploatohet gatishmëria e dobët e sistemit për reagim dhe mbi këtë bazë të bëhen manipulime dhe dezinformata. Prandaj, kjo sugjeron nevojën për zgjidhje ligjore shtesë.

Gjatë përgatitjes së këtij studimi, pas një procedure përfundimtare të Qeverisë para Kuvendit të Republikës së Maqedonisë së Veriut, u paraqit Ligji për sigurinë e rrjeteve dhe sistemeve të informimit. Rrjeti dhe sistemet e informimit, dhe mbi të gjitha interneti,

1 Që i referohet nenit 8 të Konventës Evropiane për të Drejtat e Njeriut (KEDNJ) për mbrojtjen e jetës private, reputacionit dhe nderit

luajnë një rol thelbësor në lehtësimin e veprimit keqdashës dhe zbatimin e ndërhyrjes së huaj dhe manipulimit me informacionin. Për shkak të kësaj natyre transnacionale, ndërprerjet e rëndësishme në këto sisteme, qoftë të qëllimshme apo të paqëllimshme dhe pavarësisht se ku ndodhin, gjithashtu mund të ndikojnë në Maqedoninë e Veriut. Për më tepër, ligji transpozon Direktivën (BE) 2016/1148 të Parlamentit Evropian dhe të Këshillit Evropian të 6 korrikut 2016 në lidhje me masat për një nivel të lartë të përgjithshëm të sigurisë së rrjeteve dhe sistemeve të informimit në të gjithë Bashkimin Evropian, përkatësisht Direktivën për mbrojtjen e rrjeteve dhe sistemeve të informimit të njohur si *Direktiva NIS*.[2], analiza në këtë seksion do të përqendrohet në mënyrë më të detajuar në disa nga zgjidhjet ligjore.

PËRMBLEDHJE E DISPOZITAVE TË KODIT PENAL (KP) TË REPUBLIKËS SË MAQEDONISË SË VERIUT

Në Kodin penal ka disa nene që mund të lidhen në mënyrë indirekte me ndërhyrjen e huaj dhe manipulimin me informacionet. Kështu, për shembull, neni 137 i Kodit penal vlerëson si vepër të dënueshme "Nxitja e urrejtjes, përçarjes dhe intolerancës kombëtare, racore dhe fetare" dhe gjuhës që shkakton urrejtje dhe përçarje. Megjithatë, ky artikull nuk mbulon ndikimin e aktorëve të huaj ose fushatat e organizuara për dezinformim.

Për më tepër, neni 274, i cili i referohet përgjimit të paautorizuar dhe incizimit të zërit, i referohet aktiviteteve të paligjshme që mund të jenë pjesë e NHMI-së, por nuk mbulon dezinformimin digjital ose ndërhyrjen e huaj përmes mediave.

Gjithashtu interesant është neni 394-d – Kërcënimi terrorist, i cili i referohet akteve kërcënuese për sigurinë, por nuk mbulon manipulimin psikologjik përmes informacioneve.

Për sa i përket ndërhyrjes së huaj dhe manipulimit me informacionet, Kodi penal do të duhet të zhvillohet për të adresuar ndërhyrjen e huaj dhe manipulimin me informacionet, duke përfshirë:

- përkufizim të qartë të "manipulimit të huaj me informacionet";

2 Kjo direktivë ndër të tjera insiston që Shtetet Anëtare të përmirësojnë aftësitë e tyre për siguri kibernetike me vendosjen e masave për menaxhim të rrezikut dhe kërkesa për raportim për subjektet nga sektorë të shumtë dhe vendosjen e rregullave për bashkëpunimin, shkëmbimin e informacionit, mbikëqyrje dhe zbatimin e masave të sigurisë kibernetike.

- parashikimi i sanksioneve për fushata të organizuara dezinformuese të sponsorizuara nga shtetet e huaja;
- përshtatja ndaj ekzistencës së kërcënimeve digjitale dhe hapësirës kibernetike..

PËRMBLEDHJE E SHKURTË E LIGJIT PËR MEDIA DHE LIGJIT PËR SHËRBIME MEDIATIKE AUDIO DHE AUDIOVIZUELE

Ligji për mediat (2013) rregullon subjektet mediatike dhe transparencën e pronësisë. Ligji për shërbime mediatike audio dhe audiovizuele (2018, ndryshimet 2023) rregullon funksionimin e radiodifuzerëve dhe obligon mediat për transparencë në financim. Mangësitë kryesore të këtyre zgjidhjeve ligjore janë:

- mungesa e mekanizmave për parandalimin e propagandës së huaj përmes mediave kombëtare, rajonale dhe lokale;
- mungesa e masave për mediat gjatë shpërndarjes me vetëdije të ndërhyrjes së huaj dhe manipulimit me informacionet;

PËRMBLEDHJE E LIGJIT PËR PARANDALIMIN E PASTRIMIT TË PARAVE DHE FINANCIMIT TË TERRORIZMIT

Ky ligj, ndër të tjera, rregullon monitorimin e financimit të organizatave dhe mediave. Megjithatë, duke qenë se nuk ka një përkufizim të miratuar qartë për ndërhyrjen e huaj dhe manipulimin me informacionet përmes një dokumenti strategjik, ligji nuk synon në mënyrë eksplicite zbatimin e NHMI-së. Këto janë mangësitë kryesore të Ligjit për parandalimin e pastrimit të parave dhe financimit të terrorizmit:

- nuk ka sistem për monitorimin e financimit të huaj të portaleve informative;
- nuk rregullohet financimi i platformave online, të cilat mund të shërbejnë për ndërhyrjen e huaj dhe manipulimin me informacionet.

PËRMBLEDHJE E LIGJIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Në përgjithësi, ky ligj rregullon përdorimin dhe mbrojtjen e të dhënave personale. Megjithatë, ligji nuk rregullon keqpërdorimin e të dhënave për "dezinformim të synuar" ose „operacione psikologjike", gjegjësisht operacione për ndikim. Për rrjedhojë, disavantazhet kryesore janë:

- mungesa e mekanizmave për mbrojtje nga manipulimet e huaja digjitale (siç është skenari i Cambridge Analytica ose manipulimi nga të ashtuquajturat *"kompani platforma")*[3]

- mungesa e procedurave të qarta për përgjigje ndaj operacioneve psikologjike masive, përkatësisht operacioneve për ndikim të bazuar në keqpërdorimin e të dhënave.

2.3. SHQYRTIM KRITIK: SFIDAT INSTITUCIONALE NË MAQEDONINË E VERIUT PËR PËRBALLJE ME NDËRHYRJEN E HUAJ DHE MANIPULIMIN ME INFORMACIONET

Lufta kundër ndërhyrjes së huaj dhe manipulimit me informacionet në Maqedoninë e Veriut, zhvillohet përmes një labirinti kompleks të dobësive institucionale, burimeve të kufizuara dhe strategjive të pa harmonizuara. Megjithëse ekzistojnë mekanizma dhe institucione formale që, sipas ligjeve dhe rregulloreve të tjera, janë përgjegjëse për mbrojtjen nga kërcënime të tilla, kapaciteti i tyre real për t'iu kundërvënë fushatave të koordinuara të dezinformimit mbetet shqetësues i ulët. Një problem shtesë është mungesa e emërimeve të bazuara në merita në sektorin publik.

3 Bëhet fjalë për kompani që, në vend që të prodhojnë produkte ose shërbime drejtpërdrejt, ofrojnë infrastrukturë që u lejon palëve të treta të krijojnë vlerë. "Kompanitë platformë" po transformojnë ekonominë dhe mënyrën se si njerëzit kanë qasje në shërbimet, shpesh duke sfiduar industritë tradicionale. Ato janë biznese që veprojnë si ekosisteme digjitale, që lidhin grupe të ndryshme përdoruesish (p.sh., blerës dhe shitës, shoferë dhe pasagjerë, krijues të përmbajtjes dhe konsumatorë).

Në thelb, institucionet maqedonase, si Agjencia për Siguri Kombëtare (ASK), Ministria e Punëve të Brendshme (MPB), Agjencia për Kundërzbulim (AKZ), Shërbimi Ushtarak - Sektori për Siguri dhe Kundërzbulim- (ShUSSK) pranë Ministrisë së Mbrojtjes (MM) dhe Qendra Kombëtare për Reagim ndaj Incidenteve Kompjuterike (MKD-CERT), reagojnë ndaj ndërhyrjeve të huaja dhe manipulimit të informacioneve në bazë ad hoc, pa një strategji të vetme, të centralizuar që do të mundësonte një përgjigje efektive dhe të koordinuar.

Agjencia e Sigurisë Kombëtare (ASK), e cila ka një mandat për operacionet e kundërzbulimit, në praktikë ka nevojë për një ekip të specializuar të zhvilluar që merret me dezinformatat digjitale dhe kërcënimet hibride. Në vend të kësaj, mbështetet kryesisht në metodat tradicionale të inteligjencës. Këto metoda, në kushtet e luftës moderne informative në të cilën ka edhe operacione të ndikimit, keqpërdorim të hapësirës kibernetike dhe të ashtuquajturat sulme nën "pragun e përdorimit klasik të forcës" përmes teknologjive, nuk janë më të mjaftueshme. Një sfidë më e madhe paraqet fakti se ASK nuk ka kompetenca të qarta për përballje me manipulimet në internet të opinionit publik, veçanërisht kur ato nuk janë rezultat i drejtpërdrejtë i shërbimeve të huaja të inteligjencës, por i një rrjeti para-shtetëror ose "gri" të aktorëve që përdorin mediat lokale dhe rrjetet sociale si mjete për ndikim. Pa një dokument publik për ngritjen e kapaciteteve të ASK-së në këtë drejtim, është e paqartë nëse situata po zgjidhet.

Departamenti për Krim Kibernetik i Ministrisë së Punëve të Brendshme (MPB) kryesisht merret me krime klasike kibernetike si mashtrimet financiare dhe hakerimet. Për një analizë të strukturuar të rrjeteve të dezinformimit, Sektori do të përfitonte nga staf më i trajnuar profesionalisht, ekspertë të forenzikës ligjore digjitale, mjete të sofistikuara për monitorimin e fushatave digjitale, si dhe bashkëpunim më të thellë me kompanitë globale të teknologjisë si Meta, Google dhe X.

Agjencia e Inteligjencës (AK) gjithashtu ka nevojë për kapacitete njerëzore dhe teknike. Edhe pse ka përpjekje për të ndërtuar kapacitete përmes bashkëpunimit bilateral apo multilateral, këto përpjekje nuk janë planifikuar apo financuar nga vetë agjencia, por sigurohen përmes projekteve të donatorëve.

Shërbimi ushtarak – Sektori për Siguri dhe Kundërzbulim në Ministrinë e Mbrojtjes, përballet me të njëjtat sfida. Ministria dhe Armata e Republikës së Maqedonisë së Veriut (ARMV) nuk kanë zhvilluar një doktrinë, si për zvogëlimin e rrezikut për anëtarët

e ushtrisë dhe personelit civil në forcat e armatosura dhe ministrinë dhe familjet e tyre në vend, ashtu edhe për ushtarët dhe personelin civil që janë të vendosur për të kryer detyra në misione të parapara nga NATO, BE ose OKB.

Edhe pse ekziston një autoritet ushtarak i mbrojtjes kibernetike, ai kryesisht fokusohet në mbrojtjen e infrastrukturës kritike, dhe jo që të analizojë kërcënimet hibride që përfshijnë luftën e informacionit dhe operacionet e ndikimit. Kjo është veçanërisht shqetësuese duke pasur parasysh se doktrinat moderne ushtarake të Rusisë, Kinës, por edhe grupeve terroriste me një agjendë globale, mbështeten fuqishëm në operacionet e informacionit si pjesë e strategjisë së tyre për projektim të fuqisë. Megjithëse brenda Ushtrisë operacionet psikologjike adresohen në një farë mase, e gjithë qasja është në një nivel bazë me fokus në operacionet ekspeditive të Ushtrisë, jo në kontekstin e detyrës kushtetuese për të mbrojtur integritetin dhe sovranitetin territorial. Kur kësaj i shtohet edhe kufizimi ligjor i operacioneve të Ushtrisë në territorin e shtetit, del qartë se ky kapacitet është i pamjaftueshëm për kërcënimin e NHMI-së.

Duke pasur parasysh se në kuadër të BE-së, dezinformimi ka qenë pjesë integrale e kërcënimeve kibernetike që nga viti 2023 (CERT–EU, 2024). Qendra Kombëtare e Reagimit ndaj Incidenteve Kompjuterike (NCIR) në kuadër të Agjencisë për Komunikime Elektronike duhet të forcojë vazhdimisht kapacitetet e saj njerëzore dhe kapaciteteve të tjera për të kryer funksionin e saj kryesor - trajtimin e incidenteve kibernetike dhe për të monitoruar tendencat e BE-së dhe NATO-s në këtë kontekst. Gjegjësisht, BE e sheh dezinformimin si një pjesë integrale të sigurisë kibernetike, dhe NATO që nga viti 2015 beson se hapësira kibernetike është një fushë e veçantë e luftës dhe prandaj kur planifikohet siguria kibernetike, duhet të planifikohen reagime dhe operacione për t'u marrë me operacionet e ndikimit *(Hubervic A., Prudent Y., STO)*. Për më tepër, siguria kibernetike, dhe kështu kërcënimet nga dezinformimi dhe manipulimi i ndikimit, janë pjesë e sigurisë kombëtare.[4]

Një aspekt tjetër kritik në këtë kontekst është se Agjencia për Shërbime Mediatike Audio dhe Audiovizive (AShMAA) ka autoritet mbi platformat sociale vetëm nëse ato janë të regjistruara në vend dhe nuk ka *(Ligjit për shërbime mediatike audio dhe audiovizuele, 2014)*. Qendrat e huaja dhe vendase të dezinformimit mund të shfrytëzojnë këtë boshllëk ligjor për të krijuar dhe mirëmbajtur portale që nuk kanë pronësi të përcaktuar qartë dhe që mund të zhduken dhe të rishfaqen me një emër tjetër në vetëm pak orë.

4 Për shembull, Strategjia për Mbrojtjen Kibernetike, e cila është e vjetërsuar, identifikon se neni 5 mund të jetë baza ligjore për kryerjen e operacioneve fizike ushtarake dhe përdorimin e forcës në përgjigje të sulmeve kibernetike.

Ndikimi i huaj nëpërmjet dezinformimit, si kudo tjetër, ka një peshë të veçantë në proceset zgjedhore. Prandaj, Komisioni Shtetëror Zgjedhor (KSHZ), i cili është përgjegjës për transparencën e procesit zgjedhor, duhet të përmirësojë kapacitetet e tij për monitorimin e ndërhyrjeve digjitale në zgjedhje. Përndryshe, në rastin më të keq, aktorët e huaj mund të përhapin informacion të rremë rreth proceseve zgjedhore pa u ndëshkuar, të përdorin botnet për të diskreditуar kandidatë të caktuar dhe madje të ndikojnë në rezultatet e zgjedhjeve përmes fushatave të krijuara për të dekurajuar votuesit. Në këtë kontekst, vlen të përmendet gjithashtu se portalet online të regjistruara jashtë vendit mund të marrin fonde për fushata politike në vend.

Dobësitë institucionale nuk janë vetëm pasqyrim i sfidave që vijnë nga mungesa e burimeve teknike apo njerëzore. Problemi thelbësor qëndron në mungesën e koordinimit dhe vullnetit politik për një qasje gjithëpërfshirëse për zgjidhjen e kësaj çështjeje. Maqedonia e Veriut nuk ka një qendër të veçantë kombëtare për të luftuar dezinformimin. Organeve ekzistuese që supozohet të mbulojnë këtë fushë shpesh u mungon një mekanizëm i qartë për shkëmbimin e të dhënave dhe inteligjencës ose janë jofunksionale. Kështu, për shembull, Këshilli Koordinues i Komunitetit të Inteligjencës së Sigurisë, i cili është përgjegjës për luftimin e kërcënimeve hibride, është jofunksional dhe nuk lejon shkëmbimin e informacionit në nivel institucional. Përveç kësaj, nuk ka lidhje digjitale ndërmjet institucioneve, kështu që në rast problemi, shpesh për shkak të strukturës organizative dhe pozicioneve të ndryshme të vartësisë (që është e mirë për decentralizimin dhe shmangien e akumulimit të pushtetit), nuk është e qartë se cili institucion dështon ose ka kompetencën për një problem të caktuar. Kjo krijon një vakum të rrezikshëm, të cilin aktorët e huaj mund ta përdorin për të përhapur pa pengesa narrative dhe forma të tjera ndikimi që minojnë proceset demokratike dhe sigurinë kombëtare.

Një dobësi tjetër është mungesa e iniciativave gjithnjë e më të shpeshta institucionale për rritjen e ndërgjegjësimit të publikut për ndërhyrjet e huaja dhe manipulimin e informacionit dhe edukimit informativ dhe mediatik të popullatës. Një institucion që ka mandat ligjor për promovimin e edukimit mediatik përmes bashkëpunimit me organizatat e shoqërisë civile, institucionet arsimore, mediat dhe institucionet është AShMAA. Në vitin 2017 krijoi Rrjetin e Edukimit Mediatik, tashmë me mbi 80 anëtarë (ministri, institucione shtetërore, institucione arsimore, shoqata dhe organizata qytetare dhe media) dhe një herë në vit realizon një fushatë me interes publik në bashkëpunim me median, kushtuar edukimit dhe sigurisë mediatike gjatë përdorimit të internetit dhe mediave sociale[5]. Megjithatë, një pjese të madhe të qytetarëve

5 Shih më shumë në: https://mediumskapismenost.mk/

maqedonas u mungojnë njohuritë, aftësitë dhe mjetet për të njohur narrativat manipuluese, gjë që i bën ata të cenueshëm ndaj ndikimeve nga burime të ndryshme propagandistike. Kjo situatë përkeqësohet nga fakti se disa elita politike vendase përdorin dezinformimin si një mjet për llogaritje politike, duke kontribuar, me vetëdije ose pa vetëdije, në intensifikimin e ndërhyrjes së huaj dhe manipulimin e informacionit. Afërsia e gjuhëve (serbo-kroatisht dhe shqip) është një problem shtesë që në një epokë të shoqërive të hapura dhe tregjeve të lira gjithashtu kërkon një qasje të kujdesshme.[6]

Përballë këtij realiteti, institucionet në Maqedoninë e Veriut duhet të ndërmarrin hapa vendimtarë për të përmirësuar kapacitetet dhe për të krijuar një strategji për rezistencën kombëtare ndaj ndërhyrjes së huaj dhe manipulimit të informacionit. Kjo nënkupton:

- një qasje gjithëpërfshirëse në luftën kundër dezinformimit dhe ngarkimi të një autoriteti që do të koordinojë të gjithë aktorët shtetërorë në këtë kuptim;
- forcimin e kapaciteteve të ASK, AR, MPB, ON dhe ARMV për monitorimin dhe neutralizimin e NHMI;
- rritjen e bashkëpunimit me NATO-n, BE-në dhe kompanitë e teknologjisë për t'u marrë me dezinformimin kibernetik;
- promovimi i edukimit mediatik dhe informativ në sistemin arsimor si një strategji afatgjatë për ndërtimin e elasticitetit.

Nëse këto masa nuk merren në kohë, shteti do të mbetet i prekshëm nga manipulimet e informacionit të huaj, të cilat në planin afatgjatë mund të dëmtojnë jo vetëm demokracinë, por edhe sigurinë kombëtare.

6 Aktorët e huaj ose dezinformuesit vendas që janë të okupuar, të korruptuar ose të blerë mund të përshtatin shpejt narrativat nga një gjuhë në tjetrën, ose t'i postojnë vetëm në serbo-kroatisht ose shqip. Kështu, nga një qendër (Beogradi, Tirana, etj.) mund të ndikojnë në të gjithë rajonin. Kjo mundëson shpërndarjen e koordinuar të informacionit të rremë në bashkësi të ndryshme etnike, veçanërisht nëse dihet fakti se një numër i madh i mediave lokale për shkak të kapaciteteve të pakta shpesh shkarkojnë informacione nga këto qendra. Kjo ngjashmëri gjuhësore mund të përdoret gjithashtu për të krijuar përkthime të rreme, fushata dezinformuese me citime të manipuluara ose lajme të fabrikuara që tingëllojnë autentike për grupe të shumta, por gjithashtu mund të kuptohen nga një audiencë më e madhe. Kjo është veçanërisht e rrezikshme në kontekste të ndjeshme siç janë krizat politike, zgjedhjet ose tensionet ndëretnike, ku mesazhet e manipuluara mund të nxisin mosbesimin, ndarjet dhe destabilizimin.

2.3.1. SHQYRTIMI I KAPACITETIT SHTETËROR PËR T'IU PËRGJIGJUR FUSHATAVE TË DEZINFORMIMIT

Kapaciteti shtetëror për t'iu përgjigjur fushatave të dezinformimit, si pjesa më e rëndësishme për trajtimin e ndërhyrjes së huaj dhe manipulimit me informacionin, mund të përmblidhet shkurtimisht se ai është i kufizuar në monitorim dhe analizë. Për më tepër, ekziston një kapacitet i dobët institucional në Maqedoninë e Veriut për të siguruar një përgjigje gjithëpërfshirëse të plotë dhe në kohë duke krijuar një narrativë të përshtatshme. E gjithë kjo dobësi institucionale. Në pjesën që vijon, përmes analizës së këtyre tre parametrave - kapaciteti për të monitoruar dhe analizuar dezinformimin, për të komunikuar në mënyrë strategjike dhe për të formuar një besim qytetar dhe kundër-narrativ në institucione, do të bëhet një rishikim i kapacitetit shtetëror për t'iu përgjigjur fushatave të dezinformimit.

PASQYRË E SHKURTËR E KAPACITETIT SHTETËROR PËR MONITORIMIN DHE ANALIZIMIN E DEZINFORMATAVE

Në hapësirën moderne të informacionit, dezinformimi po përhapet me shpejtësi të paparë. Algoritmet e rrjeteve sociale nxisin polarizimin dhe aktorët e huaj përdorin mediat lokale, trollet dhe botnetet për të përforcuar narracionet e tyre.

Institucionet shtetërore nuk kanë mekanizma mjaftueshëm të zhvilluar për monitorimin e ndërhyrjeve të huaja dhe manipulimit të informacionit, prandaj shpesh mbështeten në analizat e sektorit joqeveritar dhe partnerëve ndërkombëtarë. Megjithëse këto analiza janë të mira dhe të dëshirueshme, ato nuk janë të mjaftueshme në vetvete dhe nuk kanë karakter shtetëror.

Megjithëse si shtet anëtar i NATO-s, Maqedonia e Veriut merr ndihmë të madhe nga Qendra e Ekselencës për Komunikime Strategjike (NATO StratCom CoE) dhe, si një vend aspirant për në BE, nga iniciativa e BE-së për të luftuar dezinformimin EUvsDisinfo, këto mekanizma kanë vetëm rol konsultativ. Madje edhe kur partnerët e jashtëm ngrenë alarmin për sulme dezinformative që synojnë shtetin, institucionet duhet të kenë një mekanizëm të përshtatshëm reagimi. Prandaj, nevojitet një qasje institucionale për të ngushtuar hapësirën e manovrimit për aktorët keqdashës, shpesh shtetërorë dhe jo-shtetërorë.

NJË PASQYRË E KAPACITETIT KOMBËTAR PËR KRIJIMIN E NJË NARRATIVE

Në Maqedoninë e Veriut, kundërshtimi i ngadaltë dhe joefektiv ndaj fushatave të dezinformimit është i dukshëm, gjë që lë hapësirë për intensifikimin e tyre. Përveç mungesës së kapaciteteve monitoruese, institucioneve maqedonase u mungon një kundër-narrativë e qartë dhe bindëse që do t'i kundërvihej dezinformimit dhe shpesh as nuk përgjigjet shpejt, as nuk mohon ose nuk shpjegon dezinformimin. Si rezultat, të pavërtetat po përhapen në hapësirën publike me shpejtësi të madhe. Për shembull, kur Maqedonia e Veriut u gjend nën sulm të fushatave dezinformuese rreth anëtarësimit në NATO, të cilat promovuan narrativa për „burimet e vjedhura kombëtare" dhe „përfshirjen ushtarake të vendit në konflikte", institucionet nuk arritën të komunikojnë me publikun në kohën e duhur. Në vend të një qasjeje proaktive me mesazhe dhe prova të qarta, reagimi i shtetit ishte i kufizuar në deklarata të përgjithshme, pa komunikim të hartuar në mënyrë strategjike. Ka pasur një shembull të tillë në sulmin kibernetik ndaj Fondit të Sigurimeve Shëndetësore, për të cilin ka shqetësime serioze në lidhje me vjedhjen e një numri të madh të të dhënave të qytetarëve.

Një problem shtesë është se zyrtarët e qeverisë maqedonase shpesh përdorin gjuhë të komplikuar burokratike. Kjo gjuhë nuk është përshtatur dhe kështu është joefektive në epokën digjitale. Nga ana tjetër, dezinformimi është formuluar në një mënyrë të thjeshtë dhe emocionale, duke e bërë atë më të arritshme dhe me ndikim për publikun e gjerë. Ata artikulojnë emocionet, zgjojnë empatinë, sulmojnë vlerat, minojnë besimin, shpesh janë të formuar në mënyrë elegante me hiperbola, krahasime joadekuate, lënë pas dore momentet kyçe që mund të japin një rrjedhë të ndryshme në tezën e tyre të argumentit dhe theksojnë aspektet problematike që i shërbejnë qëllimeve të tyre. Edhe kur nuk ka lidhje të drejtpërdrejtë, ato nënkuptojnë çështje etnike, zhgënjime politike dhe tema historikisht problematike, përmes legjitimitetit të vetëshpallur ose të nxjerra jashtë kontekstit dhe tezave të paraqitura jo plotësisht të shkencëtarëve dhe ekspertëve të vendosur.

Një aspekt tjetër kryesor është mungesa e një njësie, departamenti ose organi për reagim të shpejtë dhe të koordinuar ndaj sulmeve dezinformuese. Në shumë vende, Trupa të tilla janë pjesë e zyrave të kryeministrave ose ministrive të jashtme. Prandaj, për shkak të kompleksitetit dhe diversitetit të fushave dhe temave përmes të cilave shpërndahet dezinformimi, shumë shpesh, bërja e deklaratave joadekuate ose jo të plota nga zyrtarët qeveritarë mund të jetë në vetvete një mundësi për manipulim dhe dezinformim. Në praktikë, gazetarët shpesh nuk kanë aftësinë për të raportuar në mënyrë adekuate sepse u mungon gatishmëria tematike dhe e ekspertëve, kështu që ata përcjellin informacione

që janë të pjesshme, shpesh të formuluara dobët dhe/ose jo plotësisht të sakta. Si pasojë, po krijohet kaos informativ që dëmton më tej kapacitetin e autoriteteve shtetërore për t›u marrë me dezinformimin, dhe kështu dhe besimin e publikut.

BESIMI I PUBLIKUT NË INSTITUCIONE SI ELEMENT PËR PËRBALLJE ME DEZINFORMATAT

Në publik shpesh mbizotëron mendimi se vetë institucionet janë burim manipulimi, gjë që e ndërlikon më tej luftën kundër ndërhyrjes së huaj dhe manipulimit me informacionet. Disa qytetarë i shohin institucionet si pjesë të problemit, jo si një zgjidhje *(Jakimova J., 2022)*. Ky mosbesim në përgjithësi lind nga disa faktorë, siç janë instrumentalizimi politik i informacionit, korrupsioni dhe abuzimi me pushtetin politik, fushatat e komunikimit të organizuara dobët dhe të pasuksesshme.[7] Në këtë kuptim, publiku shpesh dëshmon interpretime të motivuara politikisht të fakteve, gjë që zvogëlon besueshmërinë e burimeve zyrtare. Shumë qytetarë besojnë se institucionet nuk punojnë në interesin e tyre, duke i bërë ata të ndjeshëm ndaj dezinformimit. Shpesh përkthehet në praktikë se „Perëndimi kontrollon vendin“ ose se „Maqedonia e Veriut është një shtet kukull“. Së fundi, mungesa e transparenca është një mungesë e madhe që është njohur në një sërë raportesh nga organet e pavarura, por edhe nga BE-ja *(Komisioni Evropian, 2021)*. Institucionet shpesh përgjigjen duke mohuar ose injoruar tema të diskutueshme, të cilat vetëm thellojnë krizën e besimit.

7 Për shembull, është mendim i ekspertëve se pas ndryshimit të pushtetit si rezultat i skandalit të përgjimit në vitin 2017, udhëheqësit e rinj (tani opozitarë) duket se pranuan të njëjtën strategji ose shërbim të konsulencës për marrëdhëniet me publikun. E thënë thjesht, asgjë nuk ka ndryshuar në këtë pjesë. Në disa raste, raporti i BE-së për Maqedoninë e Veriut nga viti 2023 vë në dukje të gjitha këto.

2.4. ANALIZA DHE SHQYRTIMI KRITIK I ROLIT TË KOMUNITETIT LOKAL SI OBJEKTIV I NDËRHYRJES SË HUAJ DHE MANIPULIMIT ME INFORMACIONET

Komunitetet lokale në Maqedoninë e Veriut luajnë një rol kryesor, në një rrjet kompleks të dezinformatave dhe ndikimit të huaj. Ato janë gjithashtu objekt i manipulimit dhe një faktor i mundshëm i rezistencës. Fushatat e dezinformimit synojnë komunitetet lokale përmes mediave kombëtare dhe lokale, platformave sociale dhe rrjeteve të aktorëve informalë në mënyrë që të shkaktojnë mosbesim, ndarje dhe destabilizim.

Komunitetet lokale janë objektiva ideale për operacionet e ndikimit për arsyen e thjeshtë se qëllimi i operacioneve të ndikimit dhe informimit është shfrytëzimi i boshllëqeve që ekzistojnë në qeverisjen efektive të institucioneve lokale në shoqëritë demokratike. Prandaj, decentralizimi i qeverisjes dhe institucioneve hap një sërë dobësish për sigurinë e shtetit. Përkatësisht, dobësitë në menaxhimin e institucioneve lokale shfrytëzohen përmes operacioneve për manipulim. Pastaj më së shpeshti komunitetet lokale janë në vijën e parë të luftës së informacionit, sepse aktorët e huaj përdorin dallimet ekzistuese etnike, politike dhe ekonomike, por edhe ambiciet fitimprurëse të elitave lokale dhe politike për të shkaktuar paqëndrueshmëri.

Fakti që shoqëria maqedonase është multietnike, në kontekstin e të gjithë lëmshit të rrethanave (dinamika lokale dhe ambiciet gjeostrategjike), komuniteti lokal në shtet është në mënyrë të pashmangshme i prekshëm nga narrativat dezinformuese që nxisin mosmarrëveshje ndëretnike. Kanalet pro-ruse shpesh përhapin dezinformata se „Perëndimi po shkatërron vlerat tradicionale“ ose se „NATO po shtyp kulturën maqedonase“ *(Vërtetmatësi, 2023)*. Këto narrative ndërlidhen me proceset e integrimit në BE *(Stanicek B. Caprile A., 2023)* dhe defokusimin e SHBA-së nga rajoni *(CSIS, 2021)* dhe, krijon një „ndjesi të pakënaqësisë“ ose të të qenët i padëshiruar. Përforcimi i tërë këtij kolazhi janë „të vërtetat problematike sentimentale“ historike që shtyjnë një pjesë të shtetësisë etnike maqedonase drejt të ashtuquajturave narrativa politike të krahut të djathtë dhe kërkesës për kombësi të pastër etnike. Komunitetet shqiptare, në të njëjtën kohë, janë në shënjestër me histori se “shteti maqedonas nuk i mbron të drejtat e tyre”, gjë që përforcon ndjenjat separatiste *(Koldomasov A., Pylypenko A., 2024)*. Kur politizimit të këtyre çështjeve i shtohet e gjithë kjo për të fituar pikë politike dhe për të mbuluar korrupsionin, keq menaxhimin, jo transparencën dhe mungesën e llogaridhënies,

hendeku i besimit në institucione vetëm sa intensifikohet dhe zgjerohet hapësira për ndikim të huaj. Super-përforcues i gjithë kësaj situate komplekse janë edhe narrativat që ndezin çështjen e identitetit maqedonas, duke përdorur mediat lokale dhe figurat me ndikim për të nxitur mosbesimin ndaj institucioneve zyrtare *(Vatsov D. at all, 2023)*.

Komunitetet lokale, veçanërisht në qytetet më të vogla, janë të prekshme nga informacioni i rremë në lidhje me ekonominë. Narrativat e dezinformimit shpesh përhapin panik, duke pretenduar se „BE nuk bën asgjë të mirë për vendin“ ose se „investimet kineze dhe ruse janë më të besueshme dhe fitimprurëse“. Kur shpallen projekte të mëdha (për shembull, investime në infrastrukturë), fushatat e dezinformimit mund t›i paraqesin ato si „pastrim parash“ ose „shitje të interesave kombëtare“. E gjithë kjo me dobësitë dhe cenueshmëritë e përshkruara më parë minon besimin në reformat e ligjshme ekonomike *(„Në rrugën drejt Maqedonisë“, 11 janar 2025)*.

Instrumentalizimi i fesë dhe vlerave tradicionale është një fenomen kompleks shtesë që, në kontekstin e një shoqërie demokratike dhe lirisë së fesë, shfrytëzohet për ndërhyrje të huaj dhe manipulim me informacionin. Institucionet fetare në komunitetet lokale shpesh përdoren si kanale për të përhapur dezinformata të caktuara, si për qëllime të aktorëve të caktuar shtetërorë ashtu edhe jo-shtetërorë. Kjo është veçanërisht e dukshme në rrëfimet kundër komunitetit LGBTQ+, emigrantëve ose ndryshimeve në sistemin arsimor, të cilat paraqiten si „ndikimi perëndimor që shkatërron vlerat tradicionale“.

3.

ROLI I MEDIAVE DHE SEKTORIT CIVIL NË MAQEDONINË E VERIUT DHE CENUESHMËRIA NDAJ NDËRHYRJEVE TË HUAJA DHE MANIPULIMIT ME INFORMACIONET

3.1. ROLI I MEDIAS NË TRAJTIMIN E NDËRHYRJEVE TË HUAJA DHE MANIPULIMIN ME INFORMACIONET

Për më tepër, peizazhi mediatik në Maqedoninë e Veriut është kompleks dhe i mbushur me ndikime politike, ekonomike dhe të jashtme, duke e bërë atë jashtëzakonisht të ndjeshëm ndaj ndërhyrjes së huaj dhe manipulimit të informacionit. E dominuar nga mediat e kontrolluara politikisht, televizionet private të varura, platformat online me standarde të dobëta të raportimit dhe dezinformimit të përhapur në rrjetet sociale, hapësira mediatike rrit cenueshmërinë e shtetit. Mediat mund t›i nënshtrohen presioneve serioze politike, duke rezultuar në presion që minon funksionin e tyre parësor si gardian i shoqërisë. Në të njëjtën kohë, të mos jetë një shërbim i pavarur për qytetarët që do të ofrojë një platformë për zëra dhe mendime të ndryshme, duke mundësuar pluralizmin dhe pjesëmarrjen aktive të qytetarëve *(BIRN Macedonia, 2023)*.

Radiotelevizioni Kombëtar (Radiotelevizioni i Maqedonisë - RTM), si shërbimi kryesor i transmetimit publik, ka potencialin të jetë një shtyllë e rëndësishme e gazetarisë profesionale dhe të paanshme. Megjithatë, presioni politik dhe financimi i pamjaftueshëm mund të kompromentojnë rolin e tij. Megjithëse formalisht i pavarur, RTM shpesh ndikohet nga elitat e partisë *(Tuneva M., 2023)*. Mungesa e burimeve adekuate është një sfidë shtesë në punën e shërbimit publik që kufizon prodhimin e përmbajtjes cilësore gazetareske dhe gazetarisë hulumtuese në luftën kundër dezinformatave *(Shoqata e Gazetarëve të Maqedonisë, 2023)*.

Dominimi i interesave politike dhe ekonomike përfaqësohet edhe nga mediat private. Studime të ndryshme tregojnë se mediat në pronësi të grupeve të biznesit shpesh mbajnë marrëdhënie të ngushta me elitat politike. Kjo rezulton në njëanshmëri të medias, vetëcensurë dhe hapësirë të kufizuar për gazetari kritike *(Tuneva M., 2023)*. Situata është e vështirë të ndryshohet dhe mediat nuk stimulojnë hulumtime dhe gazetari të orientuar tematikisht që do të forcojnë profesionalizmin dhe qasjen, ndër të tjera, ndaj problemit të ndërhyrjes së huaj dhe manipulimit të informacionit.

Ky organizim është i përsosur për strategjitë e qendrave keqdashëse antidemokratike dhe aktorëve përfaqësues të sfiduesve të agjendës euro-atlantike. Fragmentimi në rregulloret dhe në zbatimin e zgjidhjeve ligjore dhe ndërthurja e interesave të biznesit dhe atyre politike lë hapësirë për ndikim të huaj përmes narrativave të nxitura

financiarisht. Disa analiza tregojnë se media të caktuara ka shumë të ngjarë të marrin mbështetje financiare nga qendrat e huaja të pushtetit (Rusia, Serbia, Bullgaria, Turqia, Kina), e cila pasqyrohet përmes promovimit agresiv të interesave të tyre *(Shoqata e Gazetarëve të Maqedonisë, 2023)*.

Megjithatë, kanali dhe burimi kryesor i dezinformimit është media online. Hapësira digjitale dhe mundësia e veprimit në distancë, në kushtet e autenticitetit jashtëzakonisht problematik dhe mundësia e manipulimit të identitetit dhe burimit digjital, është ndoshta segmenti më i prekshëm në strukturën e medias. Pronarët dhe mënyrat e financimit të portaleve online shpesh janë të panjohura, gjë që lë hapësirë për manipulim të lehtë. Janë këto portale që janë burimi më i madh i lajmeve sensacionaliste, informacionit të pakonfirmuar dhe dezinformimit të drejtpërdrejtë, pa përgjegjësi të qarta për përmbajtjen e publikuar. Por sistematizimi dhe kategorizimi i padiskutueshëm i këtyre mediave si problem ose shtypja e tyre në kushtet e tregjeve të hapura dhe interpretimeve të ndryshme të lirisë së fjalës është jashtëzakonisht i vështirë. Mund të çojë në gabime dhe të identifikojë mediat që nuk janë pjesë e këtyre rrjeteve sikur të ishin. Kjo situatë rrit mundësinë e kamuflimit sepse përshtatja e tyre, ndër të tjera, synon të ushqejë kaosin e informacionit. Në kushte të tilla, këto portale shndërrohen lehtësisht në robotë dhe fabrika për informacion të rremë, dhe përmes tyre organizohen fushata në rrjetet sociale (Facebook, Instagram, Tic-Toc, X), duke ndikuar ndjeshëm në opinionin publik përmes profileve të automatizuara dhe aktiviteteve të koordinuara.

Kjo na çon në një aspekt tjetër kritik ndaj rolit të mediave sociale në përhapjen e NHMI-së. Media sociale është zona më e madhe e ndikimit të pakontrolluar dhe funksionon si një katalizator për fushatat e dezinformimit, pasi anashkalon standardet tradicionale të medias dhe synon lehtësisht grupe specifike të popullsisë. Në Facebook, për shembull, ka grupe që përhapin teori konspirative të përshtatura me sukses në momente të caktuara sociale ose gjeopolitike dhe të përshtatura për problemet e brendshme ose paditurinë e elitave politike për t'u marrë me dezinformimin. Kështu, për shembull, në kohën e COVID-19, narrativat anti-vaksinuese u sollën në një kontekst politik duke glorifikuar partneritetet alternative, dhe në kohën e anëtarësimit në NATO, ato përhapën propagandë anti-NATO dhe anti-BE. Grupet telegram, nga ana tjetër, funksionojnë si komunitete të mbyllura në të cilat narrativat e dezinformimit amplifikohen pa asnjë kontroll, duke krijuar të ashtuquajturin efekt eko-qelizor të njerëzve me mendje të njëjtë, në të cilin çdo mendim i kundërt refuzohet paraprakisht, ideal për radikalizim që mund të ketë pikëpamje ekstremiste dhe të udhëzojë ose të bëjë thirrje për dhunë. E gjithë kjo, në amalgamën e politizimit të çdo segmenti të shoqërisë, ka

terren serioz në edukimin e ulët mediatik dhe informativ. Një pjesë e madhe e popullsisë nuk bën dallim midis burimeve të besueshme dhe fushatave të dezinformimit, gjë që lehtëson manipulimin *(Instituti për Studime të Komunikimit, 2024)*.

Si rezultat i këtij peizazhi mediatik, Maqedonia e Veriut është shumë e prekshme nga ndikimi i huaj dhe fushatat e dezinformimit. Kjo pasqyrohet në disa aspekte kryesore:

1. polarizimi i shoqërisë në të cilën mediat politikisht të kontrolluara dhe dezinformimi në rrjetet sociale përforcojnë mosmarrëveshjet sociale;

2. mosbesimi në institucione, me qytetarë të ekspozuar vazhdimisht ndaj informacionit të rremë dhe narrativave manipuluese, dhe besimit i tyre në media dhe burime zyrtare bie poshtë;

3. në kushtet e ndërgjegjësimit dhe kapacitetit të ulët për t›u përballur me këtë formë ndikimi, elitat politike të vendit në dhjetëra vitet e fundit nuk kanë arritur të ndërtojnë një qasje sistematike (pa strategji apo politikë goditëse) për t›u përballur me dezinformimin, i cili e lë vendin të pambrojtur; dhe

4. promovimi i qetë i interesave të huaja politike dhe ekonomike pa një filtër të veçantë të caktuar nga shteti që do të pasqyrojë rrjedhën e qartë të agjendës euroatlantike. Në këtë mënyrë, media të caktuara mund të promovojnë agjendat e vendeve të treta dhe të minojnë drejtpërdrejt politikën e jashtme të Maqedonisë dhe proceset e integrimit në BE dhe NATO.

3.2 ROLI I SHOQËRISË CIVILE NË TRAJTIMIN E NDËRHYRJEVE TË HUAJA DHE MANIPULIMIN ME INFORMACIONET

Shoqëria civile në Maqedoninë e Veriut luan një rol kritik në luftën kundër ndërhyrjes së huaj dhe manipulimit me informacionin. Megjithatë, ndoshta për shkak të qasjes arkaike ndaj qeverisjes (specifike për sistemin e mëparshëm të rolit dominues të shtetit në shoqërinë civile), sektorit civil i mungon mbështetja institucionale që do të shfrytëzonte potencialin për t’u marrë me NHMI-në. OJQ-të, shoqatat e medias dhe

ekspertët individualë janë ndër të paktët aktorë që analizojnë, ekspozojnë dhe edukojnë sistematikisht dezinformimin. Megjithatë, ndikimi i tyre është i kufizuar për shkak të disa sfidave kryesore: niveli i ulët i arsimimit mediatik, burimet e kufizuara, mbështetja e pamjaftueshme e shtetit dhe, siç u shpjegua më parë, mosbesimi në institucione.

Për më tepër, niveli i ulët i edukimit mediatik dhe informativ e bën publikun të ndjeshëm ndaj manipulimit, veçanërisht në hapësirën digjitale *(Instituti për Studime të Komunikimit, 2023),* gjë që nga ana tjetër thellon cenueshmërinë ndaj ndërhyrjes së huaj dhe manipulimit të informacionit. Në kohën e afrimit të botës digjitale dhe fizike, arsimi deri më tani nuk arrin të kapë një hap në përgatitjen dhe përshtatjen e popullsisë në hapësirën digjitale (madje as të të rinjve që janë përdoruesit më të mëdhenj të informacionit elektronik). Megjithëse ekzistojnë iniciativa për arsimimin mediatik, arsimi zyrtar duhet të prezantojë arsim më intensiv për kontrollin e fakteve, edukimit digjital dhe njohjen e propagandës. Zakonet dhe supozimet për konsumin e informacionit nga mediat tradicionale, të cilat kishin ndërtuar autoritet profesional nga e kaluara, mbi të gjitha, në aspektin e legjitimitetit dhe besueshmërisë së përmbajtjes dhe u morën "si të mirëqena", tani zbatohen edhe për konsumin e informacionit nga mediat digjitale. Xhungla digjitale, në të cilën çdokush mund të krijojë përmbajtje dhe të imponojë autoritet, në kushtet e nivelit të ulët të edukimit mediatik dhe informativ, i bën qytetarët pre të lehtë ndaj grabitqarëve ekonomikë dhe politikë. Si rezultat i kësaj papërgatitjeje, një pjesë e madhe e popullsisë ende nuk ka aftësi për të dalluar burimet e besueshme të dezinformatave (Instituti për Studime të Komunikimit, 2024), gjë që lejon qarkullimin e shpejtë të narrativave të rreme.

Paragjykimi politik është një faktor shtesë që përforcon rrezikun dhe mundësinë e dezinformimit. Publiku maqedonas është shumë i polarizuar politikisht, që do të thotë se njerëzit shpesh pranojnë informacione që konfirmojnë paragjykimet e tyre, pa kontrolluar burimet. Paralelisht me dy dobësitë e mëparshme, popullsia është e etur për sensacionalizëm dhe tolerante ndaj standardeve të ulëta gazetareske nëse përmbajtja korrespondon me përkatësinë ose interesin politik. Shumë media po nxisin dezinformimin me tituj sensacionalë dhe shkarkime të pakontrolluara të përmbajtjes së mediave sociale. Afërsia e gjuhës dhe konsumimi i informacionit nga burime dhe media nga vendet e rajonit të Ballkanit Perëndimor mund të jenë një katalizator shtesë për dezinformimin që përhapet në rajon *(Reporters Without Borders, 2024; Blue Europe, 2024)*. E gjithë kjo ndikon që qytetarët me vetëdije ose pa vetëdije të marrin pjesë në përhapjen e dezinformatave, pa pasur aftësinë për të identifikuar qëllimet që qëndrojnë pas atyre rrëfimeve.

Në mungesë të një reagimi të fortë institucional ndaj ndërhyrjes së huaj dhe manipulimit të informacionit, sektori civil merr rolin kryesor në analizimin dhe ekspozimin e dezinformimit. Organizatat joqeveritare dhe studiuesit e pavarur kanë një rol kyç për të luajtur në:

a) monitorimin dhe analizimin e dezinformatave;

b) edukimi kryesisht mediatik, megjithëse ekziston një qasje segmentale e përshtatjes së plotë dhe edukimit informantiv; dhe

c) presioni publik dhe avokimi i politikave.

Disa organizata të shoqërisë civile në Maqedoninë e Veriut po punojnë në mënyrë aktive për të rritur rezistencën e popullatës ndaj dezinformimit, veçanërisht në hapësirën digjitale, duke rritur ndërgjegjësimin për dezinformimin, i cili gjithashtu kontribuon në trajtimin e ndërhyrjes së huaj dhe manipulimit të informacionit. Megjithëse ato përbëjnë mungesën e programeve shtetërore të edukimit mediatik dhe informacionit, ato kanë ndikim të kufizuar sepse nuk janë pjesë e sistemit arsimor formal. Si rezultat i projektit të USAID-it për edukimin mediatik “Të rinjtë mendojnë”, i cili është zbatuar për katër vitet e fundit nga Instituti Maqedonas për Media, Instituti për Studime të Komunikimit dhe Forumi Arsimor Rinor, dhe në bashkëpunim me Ministrinë e Arsimit dhe Shkencës (MASH) dhe Byronë për Zhvillimin e Arsimit (BZHA), edukimi mediatik është përfshirë në arsimin fillor, në lëndët e gjuhës amtare në të gjitha vitet. Më shumë se 8000 mësimdhënës u trajnuan dhe u zhvillua një Kornizë për edukim mediatik për Arsimin fillor me qëllim të ofrimit të aftësive themelore dhe udhëzimeve të strukturuara për integrimin e edukimit mediatik në procesin mësimor. Në arsimin fillor, mësohen edhe lëndë të tjera që mbulojnë segmente të edukimit mediatik dhe aftësive për edukim digjital. Megjithatë, në arsimin e mesëm, programet mësimore mbulojnë mediat si përmbajtje, por pa një theks të veçantë në edukimin mediatik. Vetëm disa nga çështjet në lidhje me edukimin mediatik trajtohen në lëndë të ndryshme. Në arsimin e lartë, si rezultat i projektit të USAID-it në tre vitet e fundit, lëndët zgjedhore për edukim mediatik janë futur në 8 fakultete, përfshirë ato për rekrutimin e mësimdhënësve për arsimin fillor dhe të mesëm. Projekti gjithashtu kontribuoi në arsimin joformal duke hapur klube për edukim mediatik në 30 shkolla fillore dhe të mesme dhe duke organizuar trajnime dhe punëtori për media dhe gazetari për nxënës të shkollave të mesme dhe të rinj të tjerë, duke përfshirë më shumë se 2000 të rinj. Megjithatë, sipas raportit kombëtar nga Monitorimi i Pluralizmit Mediatik në Epokën Dixhitale për vitin 2023 *(Micevski I., Trpevska S., 2024)*, të kryer në shtetet

anëtare dhe kandidatët e BE-së, shkalla në të cilën edukimi mediatik është inkorporuar në arsimin formal është i pakënaqshëm, ndërsa i njëjti përfundim mund të nxirret për arsimin joformal.

Presioni publik dhe avokimi për politika janë mekanizmi i ardhshëm përmes të cilit OJQ-të përpiqen të adresojnë problemin e ndërhyrjes së huaj dhe manipulimit të informacioneve. Këto përpjekje aludojnë për transparencë në media, përmirësim të kuadrit ligjor, debate publike në bashkëpunim me mediat, etj.

Megjithatë, një nga sfidat më të mëdha të punës së organizatave të shoqërisë civile është qëndrueshmëria e përpjekjeve. Puna e tyre shpesh varet nga një cikël projekti dhe mund të mos jetë i qëndrueshëm në planin afatgjatë. Manipulimet që pasuan këtë sektor bazuar në marrëdhënie të ngushta me autoritetet lënë vend për dyshime në lidhje me pavarësinë në punën e tyre *(Klinçarski P., Gaxhovska Spasovska Z., 2024)*.

Problemi dhe disavantazhi tjetër është mungesa e mbrojtjes nga sulmet politike dhe diskreditimi. Disa OJQ që ekspozojnë dezinformatat janë shënjestra e sulmeve politike dhe mediatike, ku akuzohen se janë agjentë të huaj, gjë që, së bashku me disa nga skandalet e zbuluara të korrupsionit në këtë sektor *(Pavlovska J., 2024)*, zvogëlon besueshmërinë e tyre në sytë e publikut.

Disavantazhi dhe kufizimi tjetër është fakti se nuk ka kapacitet ose angazhim adekuat për të identifikuar rrjetet e dezinformimit dhe ndikimit duke zbatuar teknika të caktuara, të tilla si OSINT – analiza e informacioneve me karakter të hapur (burimet), mjekësia ligjore digjitale dhe analiza e algoritmeve. Praktikat e mira tregojnë se sektori civil mund të luajë një rol të rëndësishëm në hartëzimin e rrjeteve të koordinuara të boteve dhe mediave manipuluese që synojnë publikun maqedonas. Kjo tregon nevojën për një qasje ndërdisiplinore, e cila do të përfshinte ekspertë të sigurisë dhe kibernetikës, të cilët kanë jo vetëm aftësi teknike, por edhe inteligjencë të sigurisë, por edhe aftësi gjuhësore (për shembull, identifikimi i manipulimeve përmes fenomenit të ashtuquajtur “boshllëqe të të dhënave” (data voids) ose informacione minimale, me cilësi të ulët ose manipuluese nga motorët e kërkimit kur ka një kërkesë të lartë për informacione mbi një temë të veçantë, por pak burime të besueshme *(Golebiewski M., Boyd D., 2019))*.

4.

KRIMI KIBERNETIK DHE RRJETET SOCIALE SI MJETE PËR NDËRHYRJET E HUAJA DHE MANIPULIMIN ME INFORMACIONET

Përpjekjet e qëllimshme për të manipulim me informacionet nga aktorët e huaj marrin një nxitje të konsiderueshme nga përparimet teknologjike. Përhapja e platformave sociale dhe shërbimeve të komunikimit mundëson një shtrirje më të madhe të ndërhyrjes së huaj dhe manipulimit të informacionit, si dhe një kombinim të taktikave, teknikave dhe procedurave të reja dhe të larmishme.

4.1. LIDHJA E NDËRSJELLË E SULMEVE KIBERNETIKE DHE DEZINFORMATAT PËR MANIPULIM

Dezinformatat e krijuara nga aktorë të huaj të përfshirë në sulmet kibernetike konsiderohen kërcënime të rëndësishme sepse mund të përhapin softuerë të dëmshëm, të ndërhyjnë në proceset politike, të jenë të vështira për t'u zbuluar, të shkaktojnë dëm dhe të nxisin dhunë. Kriminelët kibernetikë mbledhin të dhëna përmes sulmeve të synuara kundër institucioneve, grupeve ose individëve, por gjithashtu i përdorin ato për të manipuluar informacionet dhe për shpërndarjen e tyre. Rastet e hakimit dhe keqpërdorimit të llogarive të caktuara për të siguruar legjitimitetin e përmbajtjes specifike ose për të ndarë materiale të pretenduara autentike janë vetëm disa nga shembujt që ilustrojnë marrëdhëniet midis sigurisë kibernetike dhe manipulimit të mjedisit informativ.

Fushatat e sofistikuara keqdashëse kombinojnë dezinformatat dhe sulmet kibernetike nëpërmjet:

- **Terrenit** në të cilin shpërndahen dezinformatat (rrjeti social, infrastruktura e rrjetit, shërbime për riorientim). Që dezinformatat të mund të përhapen dhe të arrijë audiencën e synuar, nevojiten tre faktorë – rrjetet sociale, mjetet dhe shërbimet dhe motivimi, ndërsa pa asnjë prej tyre, ato nuk mund të jenë „të suksesshme". Mjetet dhe shërbimet për manipulimin dhe përhapjen e mesazheve nëpër rrjetet sociale shiten në të gjithë botën. Disa janë relativisht të thjeshta (pëlqime të paguara, ndjekës, etj.), ndërsa disa janë më të pazakonta - disa shërbime janë përmes sondazheve në internet, ndërsa disa duke bindur administratorët të heqin ose ndryshojnë disa përmbajtje. Që këto mjete të jenë të dobishme, rrjetet sociale shërbejnë si një platformë për përhapjen e dezinformatave. Ndërsa njerëzit kalojnë më shumë kohë dhe informohen më shpesh nga platformat sociale, rëndësia e tyre në përhapjen e informatave të rreme nuk mund të nënvlerësohet. Megjithatë, ekziston një ndryshim midis publikimit të thjeshtë të dezinformatave dhe tërheqjes së audiencës së synuar për ta konsumuar atë. Prandaj, spamerët përdorin teknika të ndryshme për të tërhequr përdoruesit për të konsumuar informacionet e tyre. Hulumtimet e fundit tregojnë se faqet e internetit për dezinformata shpesh përdorin platforma sociale si mundësues, por gjithashtu shtrihen përtej tyre, duke përdorur infrastrukturën e rrjetit dhe riorientimin e shërbimeve në nivele të ndryshme të internetit. Së fundi, pas fushatave të dezinformimit gjithmonë ekziston pyetja

„Pse?“. Motivimi ndonjëherë është thjesht një dëshirë për përfitim monetar, ndërsa në raste të tjera mund të ndryshojë nga kriminal deri në politik.

- **Taktikat** që integrojnë dezinformatat si pjesë e paketës së sulmeve kibernetike. Dezinformatat janë bërë një komponent gjithnjë e më i zakonshëm i sulmeve kibernetike, duke shërbyer për dërgimin e softuerit keqdashës duke shfrytëzuar emocionet dhe frikën e njerëzve. Për shembull, sulmuesit përdorin „Fearware“, një nëngrup i mashtrimeve për vjedhjen e të dhënave të njohura si fishing - phishing, të cilat mbështeten në shqetësimin dhe dezinformatat, të cilat u bënë veçanërisht të përhapura gjatë dhe pas pandemisë Covid-19. Për më tepër, ekziston një mbivendosje e konsiderueshme në fushatat për dezinformata dhe taktikat e krimit në internet, siç janë transaksionet e paligjshme në Darknet (një pjesë e internetit në të cilin qasja sigurohet duke përdorur softuer të veçantë), përdorimi i dokumenteve të siguruara në mënyrë të paligjshme dhe forma të ndryshme të mashtrimit.

- **Objektivat** që rezultojnë viktimat e sulmeve kibernetike njëkohësisht të jenë viktima të dezinformatave. Fushatat e dezinformimit dhe sulmet kibernetike mund të shkaktojnë lloje të ngjashme të dëmit, madje mund të kombinohen për të synuar të njëjtat viktima. Ndërsa vjedhja e të dhënave mund të kompromentojë sigurinë duke ekspozuar informacione të ndjeshme, manipulimi i këtyre të dhënave mund të ketë gjithashtu efekte të ngjashme.

- **Mundësitë** përkatësisht opsionet fitimprurëse si për fushatat e dezinformimit ashtu edhe për sulmet kibernetike. Aktivitetet e hakerimit, krimit kibernetik dhe ndikimit shpesh përdorin profesionistë të aftë siç janë burimet e jashtme, të cilët marrin stimuj të mëdhenj financiarë. Ndërsa mbrojtja kundër sulmeve mund të forcohet me softuer të ndryshëm komercial, strategjitë e dezinformimit mund të përdoren për të dëmtuar reputacionin dhe për të gjeneruar fitime. Aktualisht nuk ka dënime të rënda për aktivitete të tilla për shkak të kompleksitetit të hulumtimit të tyre dhe mungesës së masave të duhura përkufizimin dhe bllokimin e tyre.

Fushatat e dezinformimit kryhen më shpesh përmes rrjeteve sociale, sepse janë teorikisht më të vështira për t’u zbuluar sesa platformat e mediave sociale, ndërsa secila fushatë përfshin mjete specifike, si ndjekësit e blerë, pëlqimet, ripostimet, komentet, videot, etj. Pjesa më e madhe e informacioneve mashtruese rrjedhin nga teoritë e konspiracionit ose ideologjitë politike ose grupore. Shembuj të tillë janë si më poshtë:

Gjatë fushatës presidenciale të vitit 2016, Donald Trump publikoi statistikat për krimin në Shtetet e Bashkuara sipas të cilave përqindja e të bardhëve të vrarë nga të bardhët ishte 16%, dhe e të bardhëve të vrarë nga zezakët ishte 81%, ndërsa në realitet numrat ishin të kundërt, përkatësisht rreth 16% e të bardhëve u vranë nga zezakët.[8]

Jada Fransen, nënkryetare e partisë britanike të krahut të djathtë "Britania e Para", postoi një video me titullin: "Emigranti mysliman rreh djalin holandez me paterica!". Presidenti i atëhershëm amerikan Trump ndau videon, por pak më vonë ambasada holandeze publikoi me fakte se autori i aktit të dhunshëm të kësaj video është me origjinë nga Holanda.[9]

Natural News, një faqe interneti që zakonisht merret me teoritë e konspiracionit, raportoi se "vaksinat që përmbajnë merkur janë një 'gjenocid mjekësor' që synon komunitetet me ngjyrë për të dëmtuar foshnjat e tyre". Duke manipuluar artikuj të vërtetë, ata u përpoqën të ndikojnë në opinionin publik.[10]

Seattle Tribune një faqe interneti për informacione të rreme që shkarkonte dhe ndryshonte përmbajtje nga faqet e ligjshme të internetit, ndau një histori të rreme për "një nënë nga Idaho e dënuar me burg për ushqyerje me gji." Kjo histori u shpërnda në rrjetet sociale dhe nxiti diskutime në lidhje me ushqyerjen me gji në publik.

8 Shih më shumë në: https://www.washingtonpost.com/news/the-fix/wp/2015/11/22/trump-retweeted-a-very-wrong-set-of-numbers-on-race-and-murder/

9 Shih më shumë në: https://www.pbs.org/newshour/politics/trump-retweets-anti-muslim-videos-from-british-far-right-leader

10 Shih më shumë në: https://pmc.ncbi.nlm.nih.gov/articles/PMC9359307/

Fushatat e dezinformimit promovuan lajme të rreme se teknologjia 5G ndikon në sistemin imunitar dhe se brezat e spektrit 5G përhapin Covid-19.[11]

Informacioni i rremë në lidhje me trajtimet për Covid-19 ende qarkullon në rrjetet sociale, shumë prej të cilave bëjnë sugjerime të dëmshme dhe se përdorimi i barnave të paligjshme mund të "kurojë" virusin.[12]

4.2. KRIMI KIBERNETIK DHE DEZINFORMATAT SI RREZIK PËR SEKTORIN EKONOMIK

Informacioniet e rreme mund të paraqesin gjithashtu rreziqe të rëndësishme kibernetike për sektorin ekonomik, të cilat mund të rrisin ndikimin e informacionit të rremë, të ndryshuar nëse ka të bëjë me më shumë fusha të jetës shoqërore. Llojet e zakonshme të informacionit të rremë dhe rreziqet kibernetike për të cilat bizneset duhet të jenë të vetëdijshme janë:

- **e-mesazhe për fishing (phishing)**, përkatësisht e - mesazhe që duket se janë nga një burim i besueshëm për të mashtruar pranuesin e mesazhit të klikojë në një link keqdashës ose të shkarkojë softuer me qëllim të keq. Përdoruesit gjithashtu mund të mashtrohen duke klikuar në linqe qëllimkeqe, të shkarkojnë softuer keqdashës ose të zbulojnë informacione të ndjeshme përmes postimeve në mediat sociale ose llojeve të tjera të informatave të gabuara. Bizneset mund ta zbusin këtë rrezik duke zbatuar masa të forta të sigurisë së postës elektronike, siç janë filtrat për spam dhe trajnimin e punonjësve se si të identifikojnë dhe shmangin mesazhet mashtruese në emailet e tyre.

11 Shih më shumë në: https://www.bbc.co.uk/bitesize/articles/zbw492p

12 Shih më shumë në: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en

- **softuer keqdashës për bllokimin e të dhënave (ransomeware)**, të cilat janë lloje të softuerit keqdashës që mund të infektojë rrjet ose pajisje. Kjo përfshin manipulimin e sinjaleve vizuale në ndërfaqet e përdoruesit për të mashtruar përdoruesit të klikojnë një buton ose të shënojnë informacione në një formë. Pasi të instalohet, softueri keqdashës mund të vjedhë të dhëna ose të bllokojë sistemet.

- **faqe interneti të rreme ose profile të mediave sociale që përmbajnë softuer keqdashës.** Kështu, reklamat e rreme përdoren për të mashtruar përdoruesit që të shkarkojnë softuer keqdashës në pajisjet e tyre. Kështu, shfrytëzohen paragjykimet njerëzore, siç është tendenca për t›i besuar autoriteteve ose për të ndjekur turmën, shfrytëzohen për të ndikuar në vendimin të vizitohen lokacione të ueb faqeve të rreme. Nga ky këndvështrim, bizneset duhet të zbatojnë protokolle të forta të sigurisë kibernetike, siç janë verifikimi i identitetit me dy faktorë dhe kufizime për qasje, firewall, programe antivirus, përditësime të rregullta të softuerit dhe trajnim të punonjësve mbi praktikat më të mira të sigurisë kibernetike. Masa të ngjashme paraprake mund të zbatohen për të shmangur spiunazhin kibernetik, ku sulmuesit përdorin informacion të rremë për të mbledhur inteligjencë ose për të kompromet uar sigurinë.

- **sulmet e inxhinierisë sociale**, si vjedhja e të dhënave dhe vjedhja e identitetit, përkatësisht manipulimi i përdoruesve për të zbuluar informacione të ndjeshme, të dhëna për hyrje ose të dhënat financiare. Shembull për këtë është një mashtrim financiar që mund të promovojë skema mashtruese të investimeve ose mashtrime me kriptovaluta, duke bërë që përdoruesit të dërgojnë para ose kriptovaluta në llogari të rreme. Kjo mund të bëhet përmes thirrjeve të rreme telefonike, faqeve të rreme për hyrje, mesazh me email për fishing ose mesazhe në rrjetet sociale që duket se janë nga një burim i besueshëm. Për të shmangur inxhinierinë sociale, bizneset duhet të ofrojnë trajnime të rregullta për punonjësit se si të identifikojnë dhe shmangin raste të tilla.

4.3. MEKANIZMA PËR SIGURI KIBERNETIKE DHE MBROJTJE NGA DEZINFORMATAT

Përhapja e qëllimshme e informacioneve të rreme me qëllim për të manipuluar opinionin publik ose për të shkaktuar dëm, që zakonisht paraqiten si fushata dezinformuese, mund të dëmtojë sigurinë dhe reputacionin e një institucioni, grupi ose individëve.

Qeveritë, kompanitë dhe përdoruesit po bëhen gjithnjë e më të vetëdijshëm për kërcënimet e tilla. Agjenci të ndryshme qeveritare, tani po krijojnë shërbime për zbulimin e informacioneve, për të cilat besojnë se janë të rremë. Ata po konsiderojnë gjithashtu vendosjen e rregulloreve dhe ndëshkimin e faqeve që publikojnë dezinformata. Qëllimet e rregulloreve të reja do të përfshijnë mundësinë për të pezulluar përdoruesit e bot/ përdoruesve të dyshimtë dhe krijimin e shërbimeve që do t'i lejojnë përdoruesit të raportojnë informacione të rreme. Megjithatë, në fund të fundit, gjëja më e rëndësishme është edukimi i duhur i të gjithë përdoruesve se si të identifikojnë informacionet e rreme.

Përgjigjet potenciale për përballje me kërcënimet kibernetike mund të jenë:

- rritja e rolit të sigurisë kibernetike në identifikimin, hetimin dhe parandalimin e ndërhyrjeve të huaja dhe manipulimit të informacioneve;
- raportimi i strukturuar i incidenteve ndërmjet subjekteve përgjegjëse për sigurinë kibernetike dhe ndërhyrjen e huaj dhe manipulimin me informacionet;
- shkëmbimi i informacioneve dhe shkëmbimi i praktikave më të mira;
- promovimi dhe lehtësimi i bashkëpunimit ndërmjet institucioneve dhe organeve në nivel shtetëror;
- rritja e ndërgjegjësimit dhe mbështetja e ndërtimit të kapaciteteve.

Megjithëse zbulimi i dezinformatave mund të jetë një detyrë komplekse, ekzistojnë disa teknika dhe taktika që mund të përdoren për të identifikuar fushatat e mundshme të dezinformimit dhe të ndërmerren veprimet e duhura për zbutjen e rreziqeve, siç janë:

- vendosja e sinjalizimeve në mediat sociale dhe burime të tjera lajmesh për çdo shenjë të përhapjes së informacioneve të rreme, zakonisht nëpërmjet përdorimit të fjalëve kyçe dhe frazave që mund të lidhen me dezinformimin;

- verifikimi i çdo informacioni që shpërndahet duke kontrolluar besueshmërinë e burimit dhe duke shqyrtuar provat e paraqitura për të mbështetur pretendimet që bëhen;

- angazhimi i të gjitha palëve të interesuara për të identifikuar çdo informacion të rremë që shpërndahet dhe të zgjidhen të gjitha shqetësimet ose çështjet që mund të paraqiten;

- kryerja e vlerësimit të rrezikut për të vlerësuar ndikimin e mundshëm të fushatës së dezinformimit, i cili do të ndihmojë në përgatitjen e një përgjigje të përshtatshme;

- bashkëpunim me ekspertë të sigurisë kibernetike, marrëdhënieve me publikun dhe menaxhim të krizave për të zbuluar, menaxhuar në mënyrë efektive rreziqet dhe për t'iu përgjigjur fushatës së dezinformimit.

4.4 KËSHILLA PËR MBROJTJE NGA KËRCËNIMET KIBERNETIKE

Kushdo që është aktiv në internet rrezikon të marrë ose të transmetojë informacion të rremë ose të jetë viktimë e vjedhjes së identitetit ose llojit tjetër të keqpërdorimit ose krimit kibernetik. Çdo informacion që postohet ose shpërndahet në internet nuk zhduket kurrë, nuk mund të hiqet plotësisht dhe mund të jetë subjekt ose objektiv i keqpërdorimit. Edhe pse përdoren cilësime të ndryshme të privatësisë, kjo nuk do të thotë domosdoshmërisht se të dhënat personale janë gjithmonë të sigurta. E gjithë kjo jo vetëm që mund t'i vendosë njerëzit në rrezik online dhe fizik, por gjithashtu mund të përdoret për të krijuar dhe përhapur mesazhe dhe programe keqdashëse. Një shembull se ku kriminelët kibernetikë shpesh shkojnë për të gjetur informacione të rëndësishme për individë të caktuar është platforma sociale LinkedIn. Kjo faqe e

rrjeteve sociale mund t'i sigurojë një krimineli të mundshëm emrat e punonjësve, pozicionet e punës, përgjegjësitë e punës, madje edhe sa kohë punonjësi ka punuar në organizatë. Ky informacion mund të përdoret më pas nga kriminelët për të targetuar punonjësit me "rrezik të lartë", madje të përdoret si pjesë e një fushate më të madhe për inxhinieri sociale. Meqenëse i gjithë ky informacion tani është në dispozicion të publikut, njerëzit duhet të jenë të vetëdijshëm dhe të edukuar për rreziqet e publikimit dhe shkëmbimit të informacioneve, zbulimit të detajeve të ndjeshme për veten ose ndonjë organizatë, dhe natyrisht të jenë në gjendje t'i përgjigjen aktiviteteve potencialisht keqdashëse dhe inxhinierisë sociale.

Në përgjithësi, ka dy mënyra se si hakerat dhe kriminelët kibernetikë përdorin inxhinierinë sociale për të keqpërdorur rrjetet sociale:

1. Përpjekja për të bërë dikë të instalojë softuer në një kompjuter ose telefon që do t'i lejojë qasje në atë pajisje.

2. Për të fituar besimin e dikujt për një lloj tjetër manipulimi përmes rrjeteve sociale.

Njerëzit janë lidhja më e dobët në sigurinë kibernetike dhe çdo haker do të përfitojë nga kjo sa herë që të jetë e mundur. Këto janë disa nga mënyrat më të zakonshme që përdoren nga kriminelët kibernetikë:

- mospërdorimi i cilësimeve të duhura të sigurisë në faqet e platformave sociale. Për shembull, ndarja e lokacionit, mos kufizimi i personave që kanë qasje në informacione të caktuara, etj.;

- zbulimi i informacioneve personale, bankare ose të dhëna të tjera financiare në rrjetet sociale, duke përfshirë datën e lindjes, numrin e telefonit, adresën, llogarinë bankare. Nëse shkëmbehen këto informacione, duhet të bëhet përmes mesazheve private ose postës elektronike;

- kontakt nga të huaj nga vende të tjera. Shpesh, mashtruesit përpiqen të njohin viktimën, dhe pastaj do ta mashtrojnë. Kjo ndodh shpesh me internet faqet për takime. Ata mund të përdorin inxhinierinë sociale për të bindur se kanë nevojë për para, por gjithashtu mund të përdorin viktimën për të përhapur softuerë keqdashës ose informacione të rreme;

- me rritjen e popullaritetit të shërbimeve për mesazhe private që janë pjesë e mediave sociale, si Facebook messenger, dërgohen mesazhe private me link pa sqarim ose kanë përshkrim të paqartë për atë që përmban linku;

- ofrimi i një oferte jorealiste. Kriminelët kibernetikë përdorin ngjarjet dhe lajmet e njohura si karrem për t'i bërë njerëzit të hapin emailin e infektuar, të vizitojnë faqet e internetit të infektuara, të dhurojnë për bamirësi të rreme ose të blejnë sende që ose nuk ekzistojnë ose janë të falsifikuara;

- mos ndryshimi i fjalëkalimeve për rrjetet sociale. Hulumtimet tregojnë se një numër i madh i keqpërdorimeve janë për shkak të ripërdorimit të fjalëkalimeve dhe të dhënave të vjedhura për hyrje – 53% e përdoruesit e rrjeteve sociale nuk i kanë ndryshuar fjalëkalimet e tyre për më shumë se një vit, ndërsa 20% nuk i kanë ndryshuar kurrë. Është e këshillueshme që kjo të bëhet më shpesh.

Së fundi, vetëm duke rritur ndërgjegjësimin e publikut dhe edukimin mediatik dhe informativ të qytetarëve mund të arrihet përdorimi i duhur i platformave sociale dhe infrastrukturës së rrjetit dhe vlerësimi i mirë i përmbajtjes, në mënyrë që të parandalohet keqpërdorimi dhe manipulimi me informacionet.

5.

PËRMBLEDHJE E SHKURTËR E PRAKTIKAVE TË MIRA EVROPIANE NË TRAJTIMIN E NDËRHYRJEVE TË HUAJA DHE MANIPULIMIT ME INFORMACIONET

Për të siguruar një udhërrëfyes se si Maqedonia e Veriut mund të adresojë ndërhyrjen e huaj dhe manipulimin me informacionet, ky studim ofron një pasqyrë të shkurtër të praktikave të mira evropiane. Duhet të jetë një nxitje shtesë, por edhe një kornizë që do të lejojë një qasje holistike ndaj këtij fenomeni dhe do të zvogëlojë presionin nga NHMI që kërcënon procesin demokratik, stabilitetin institucional dhe diskursin publik.

5.1. PRAKTIKAT E SUKSESSHME NË DISA VENDE TË BE-SË

Ajo që i veçon vendet e suksesshme në këtë fushë është qasja e tyre sistematike dhe shumëdimensionale, e cila përfshin tre aspekte kryesore: (1) kuadri rregullator, (2) kapaciteti institucional dhe (3) ndërgjegjësimi i publikut dhe edukimi mediatik dhe informativ. Kjo qasje mundëson trajtimin më efikas të ndërhyrjes së huaj dhe manipulimin me informacionet përmes parandalimit, zbulimit të hershëm dhe reagimit të shpejtë institucional.

5.1.1 FORCIMI I REAGIMIT INSTITUCIONAL: MODELE TË SUKSESSHME

Në vendet që kanë arritur të ndërtojnë një mekanizëm efektiv mbrojtës kundër ndërhyrjes së huaj dhe manipulimit me informacionet, institucionet luajnë një rol kyç jo vetëm në monitorimin, por edhe në ekspozimin aktiv të dezinformatave.

Finlanda, për shembull, është e njohur për modelin e saj gjithëpërfshirës të mbrojtjes, ku agjencitë e sigurisë, mediat, organizatat e shoqërisë civile dhe institucionet arsimore punojnë ngushtë së bashku. Qeveria e Finlandës, përmes Agjencisë së Sigurisë dhe Furnizimit (Huoltovarmuuskeskus - HFK), zhvillon rregullisht vlerësimet e rrezikut dhe strategjitë për trajtimin e kërcënimeve të huaja informative. Ky model tregon se një nga pikat kryesore për ndërtimin e rezistencës sociale është analiza e vazhdueshme dhe informimi i publikut për kërcënimet e mundshme.

Një qasje e ngjashme zbatohet nga Suedia, e cila në vitin 2022 themeloi Qendrën për Mbrojtje Psikologjike (MPF). Ky organ ka për detyrë të monitorojë në mënyrë aktive, të analizojë dhe të bëjë rekomandime për trajtimin e sulmeve të huaja informative. Duke pasur parasysh se Maqedonisë së Veriut i mungon një përgjigje e koordinuar institucionale dhe një njësi e veçantë që merret në mënyrë sistematike me ndërhyrjen e huaj dhe manipulimin me informacionet, ky model mund të jetë veçanërisht i rëndësishëm.

Nga ana tjetër, Republika Çeke, pas përvojës së fushatave të intensifikuara dezinformuese në vitin 2017, krijoi një njësi të veçantë për të luftuar kërcënimet hibride në kuadër të Ministrisë së Punëve të Brendshme. Kjo njësi përbëhet nga ekspertë të fushave të ndryshme, duke përfshirë përfaqësues të shërbimit informativ, gazetarë,

ekspertë të sigurisë së TI-së dhe psikologë. Një qasje e tillë drejt ndikimit mbi operacionet ose kërcënimet hibride jep këndvështrime të ndryshme për të njëjtin problem që i lejon Republikës Çeke t›i përgjigjet shpejt dhe në mënyrë efektive dezinformatave dhe formave të tjera të ndikimit të dëmshëm të huaj.

Për Maqedoninë e Veriut, këto modele tregojnë për domosdoshmërinë e një strukture të veçantë institucionale, e cila do të jetë përgjegjëse për monitorimin, analizimin dhe përgjigjen ndaj dezinformatave. Ky institucion duhet të ketë edhe një mandat për bashkëpunim me mediat dhe organizatat e shoqërisë civile.

5.1.2 KUADRI RREGULLATOR: SI MUND TA MBROJË LIGJI DEMOKRACINË?

Përveç kapacitetit institucional, rregullimi luan një rol kyç në kufizimin e ndikimit të ndërhyrjes së huaj dhe manipulimit me informacionet. Në disa vende evropiane, ligjet janë ndryshuar për të rritur transparencën e financimit mediatik, për të vendosur kritere të qarta për funksionimin e rrjeteve sociale dhe për të sanksionuar ata që përhapin qëllimisht dezinformata.

Në Francë, për shembull, në vitin 2018, u miratua Ligji për manipulimin e informacioneve, i cili lejon institucionet shtetërore të kërkojnë që platformat sociale, të tilla si Facebook dhe X, të heqin përmbajtjet e rreme gjatë zgjedhjeve. Me këtë, fushatat dezinfomruese nuk kanë kohë të mjaftueshme të përhapen dhe të ndikojnë mbi trupin votues.

Në Lituani, ndërkohë, është në fuqi një ligj që kufizon transmetimin e mediave të huaja nëse ato identifikohen si mjete propagandistike. Qeveria ofron mbështetje financiare për mediat e pavarura, duke zvogëluar kështu varësinë e tyre nga burimet e jashtme të financimit që mund të jenë të motivuara politikisht, përkatësisht të bien në grackën e shfrytëzimit të shoqërive të hapura dhe fshehjes së shërbimeve të huaja pas investimeve financiare fitimprurëse.

Maqedonia e Veriut në këtë kontekst duhet të shqyrtojë një kornizë ligjore që do të rrisë transparencën e pronësisë së mediave, veçanërisht në portalet online, do të forcojë kapacitetet për monitorimin e propagandës në internet, do të kontribuojë në qëndrueshmërinë dhe pavarësinë e mediave dhe do të sigurojë mekanizma të veçantë për trajtimin e dezinformatave në prag të zgjedhjeve.

5.1.3 NDËRGJEGJËSIMI I PUBLIKUT DHE EDUKIMI MEDIATIK: NJË LINJË KYÇE E MBROJTJES

Siç tregojnë përvojat e Finlandës dhe Letonisë, një nga mbrojtjet më të forta kundër ndërhyrjes së huaj dhe manipulimit të informacionit është arsimi. Finlanda ka inkorporuar edukimin mediatik si pjesë e detyrueshme e sistemit arsimor dhe profesorët marrin trajnime të specializuara për të edukuar dhe arsimuar nxënësit se si të analizojnë lajmet, informacionet dhe të njohin teknikat manipuluese. Në Letoni, ndërkohë, shteti financon fushata kombëtare për edukimin mediatik, të cilat përfshijnë ligjërata online, video materiale dhe punëtori për gazetarë, mësimdhënësit dhe studentët.

Në Maqedoninë e Veriut, në këtë fushë ka ende vend për zhvillim. Qasja për forcimin e ndërgjegjësimit kombëtar në përgjithësi reduktohet në edukimin mediatik dhe varet kryesisht nga iniciativat e sektorit civil, përkatësisht donatorët. Nëse shteti ndjek shembullin e Finlandës, edukimi mediatik mund të bëhet një mekanizëm sistematik për të zvogëluar ekspozimin ndaj dezinformatave, dhe kështu ndaj manipulimit dhe ndikimit të huaj, një prirje specifike veçanërisht në mesin e popullatës së re.

****

Sidoqoftë, në zbatimin e këtyre masave, Maqedonia e Veriut duhet të jetë e vetëdijshme për ekuilibrin demokratik midis të drejtave individuale dhe sigurisë dhe mirëqenies publike. Zbatimi i disa prej këtyre masave mund të ketë lehtësisht efektin e kundërt. Zbatimi i gabuar i masave të tilla mund të çojë në rrezikimin e lirive dhe të drejtave dhe të jetë bazë për absolutizmin.

Ligji francez për manipulimin e informacioneve, për shembull, megjithëse lejon heqjen e shpejtë të informacionit të rremë, në të njëjtën kohë krijon mundësinë e censurës selektive, veçanërisht nëse institucionet që kontrollojnë këtë rregullore janë nën ndikim politik. Në Maqedoninë e Veriut, ekziston një nivel i ulët i besimit në institucione dhe politizim serioz i pothuajse çdo sektori, gjë që rrit rrezikun që mekanizma të tillë të përdoren si një mjet për çrrënjosjen e kundërshtarëve politik në vend që të kundërshtojnë me të vërtetë ndërhyrjen e huaj dhe manipulimin me informacionet.

Për më tepër, modelet që përfshijnë rregullimin shtetëror të hapësirës mediatike, siç është ai në Lituani, ku media të caktuara ndalohen për shkak tët mbrojtjes nga propaganda, mund të shkaktojnë efekt të kundërt. Kështu, në rastin e inxhinierisë politike nga një parti në pushtet, në vend që të forcojë besimin në institucione, mund të zvogëlohet lehtësisht ose të humbasë. Nëse zvogëlohet transparenca ose nëse

bëhet përzgjedhja e partive, qytetarët, së bashku me opozitën, mund t'i perceptojnë lehtësisht masat e tilla si censurë. Në Maqedoninë e Veriut, ku publiku tashmë është skeptik për politikat e qeverisë në sektorin e medias, krijimi i mekanizmave për të kufizuar burime të caktuara mund të çojë në polarizim shtesë dhe të krijojë hapësirë për kanale alternative, madje edhe më radikale të dezinformimit. Pikërisht një rezultat i tillë mund të intensifikojë fushatën e ndikimit dhe të ushqejë të gjithë kaosin informativ, në të cilin ndërhyrja e huaj dhe manipulimi i informacionit do të ndikojnë në minimin e besimit në proceset dhe institucionet demokratike, ndërsa praktikat e këqija të elitave në pushtet do të barazohen me politikat e BE-së dhe NATO-s.

Së fundi, krijimi i një organi qendror për luftë kundër dezinformatave, nëse nuk është mjaftueshëm i pavarur dhe transparent, mund të gjenerojë vetëm një pikë të re të ndërhyrjes së huaj dhe manipulimit me informacionin. Nëse Maqedonia e Veriut nuk i kushton vëmendje paanshmërisë institucionale, atëherë në vend të mekanizmave të tillë që ndihmojnë në zvogëlimin e ndikimit të dezinformatave, ato mund të bëhen një burim tjetër i mosbesimit, duke komplikuar më tej luftën kundër NHMI-së. Për të shmangur këtë rrezik, është e nevojshme që këto politika të zhvillohen përmes një procesi të gjerë konsultimi me ekspertë, mediat dhe shoqërinë civile, në vend që të jenë ekskluzivisht nën ombrellën e institucioneve shtetërore.

5.2. PËRMBLEDHJE E PRAKTIKAVE DHE PËRVOJAVE TË MIRA TË BE-SË DHE NATO-S NË PËRBALLJEN ME NDËRHYRJEN E HUAJ DHE MANIPULIMIN ME INFORMACIONET

Vitet e fundit, BE dhe NATO janë bërë të vetëdijshëm për pasojat serioze të ndërhyrjes së huaj dhe manipulimit të informacionit mbi sigurinë e tyre, stabilitetin politik dhe proceset demokratike. Kërcënimet hibride, veçanërisht fushatat e dezinformimit të udhëhequra nga aktorë të huaj shtetërorë dhe jo-shtetërorë, kërkonin një përgjigje sistematike dhe të koordinuar. Si rezultat, janë zhvilluar disa mekanizma kryesorë për trajtimin e NHMI-së, të cilat sot janë ndër shembujt më të suksesshëm në përgjigjen globale ndaj kërcënimeve informative. Ky studim ofron një përmbledhje të tre prej

iniciativave më domethënëse: Task Forca e Komunikimit Strategjik – BE Lindje (East StratCom Task Force) (BE), Qendra Hibride e Ekselencës (Finlandë) (Hybrid Center of Excellence) dhe Sistemi për Alarmim të Shpejtë (BE) (Rapid Alert System), dhe thekson mësimet që Maqedonia e Veriut mund të nxjerrë prej tyre.

5.2.1.TASK FORCA PËR KOMUNIKIM STRATEGJIK - LINDJE E BE-SË (EAST STRATCOM TASK FORCE)

Task Forca për Komunikim Strategjik (East StratCom Task Force) është fronti i parë i organizuar kundër dezinformatave. I themeluar në vitin 2015 në kuadër të Shërbimi Evropian për Veprim të Jashtëm (European Union External Action-EEAS), përfaqëson përpjekjen e parë të BE-së për trajtim sistematik të dezinformatave, veçanërisht ato që vijnë nga Federata Ruse. Qëllimi kryesor i këtij organi është të identifikojë, analizojë dhe ekspozojë narrativat e dezinformimit, por edhe të forcojë kapacitetet e komunikimit të BE-së në fqinjësinë lindore.

Ky mekanizëm mbështetet në tre shtylla veprimi, si më poshtë:

1. Komunikimi proaktiv i BE-së në fqinjësinë lindore – duke krijuar dhe shpërndarë informacion të saktë dhe të verifikuar, East StratCom punon për të forcuar narrativën pozitive të BE-së. Kjo veçanërisht vlen për vende si Ukraina, Gjeorgjia dhe Moldavia, të cilat shpesh janë objekt i propagandës anti-BE.

2. Monitorimi dhe ekspozimi i dezinformatave – ekipi menaxhon platformën EUvsDisinfo, e cila monitoron dhe ekspozon narrativat e dezinformatave. Nëpërmjet një analize të detajuar, platforma etiketon informacione të rreme, shpjegon se si përhapet dhe ofron korrigjime faktike.

3. Forcimi i edukimit mediatik dhe qëndrueshmërisë së shoqërive - East StratCom bashkëpunon me mediat lokale, organizatat e shoqërisë civile dhe ekspertët, duke ofruar trajnime për kontrollin e fakteve, mjete analitike dhe udhëzime për zbulimin e dezinformatave.

Më poshtë janë mësimet kryesore për Maqedoninë e Veriut nga ky mekanizëm i BE-së:

- nevoja për një qasje të koordinuar midis institucioneve shtetërore dhe sektorit joqeveritar për monitorim të dezinformatave;

- zhvillimi i një platforme kombëtare për të ekspozuar manipulimin dhe ndërhyrjen përmes informacioneve të huaja (ngjashëm me EUvsDisinfo); dhe
- investimi në komunikimin profesional të institucioneve shtetërore për të zvogëluar hapësirën për manipulim.

5.2.2. QENDRA E EKSELENCËS PËR KËRCËNIMET HIBRIDE (HYBRID CENTER OF EXCELLENCE): MBROJTJA HIBRIDE PËRMES ANALIZËS DHE KOORDINIMIT STRATEGJIK

Qendra e Ekselencës për Kërcënimet Hibride (Hybrid CoE), e themeluar në Finlandë në vitin 2017, përfaqëson një nga përpjekjet më komplekse për të trajtuar kërcënimet hibride, duke përfshirë ndërhyrjen e huaj dhe manipulimin me informacionet. Kjo qendër funksionon si një platformë për shkëmbimin e informacioneve, analizës dhe ekspertizës midis NATO-s dhe shteteve anëtare të BE-së.

Ndryshe nga East StratCom, e cila synon dezinformata specifike, Qendra e Ekselencës për Kërcënimet Hibride ka një mision më të gjerë, duke analizuar të gjitha aspektet e kërcënimeve hibride, siç janë presionet ekonomike, sulmet kibernetike dhe manipulimi i zgjedhjeve. Qendra funksionon përmes tre platformave kryesore, si më poshtë:

1. Analiza e kërcënimeve hibride dhe ndërhyrjes së huaj dhe manipulimit me informacionet – Qendra publikon studime dhe parashikime të hollësishme se si zhvillohen strategjitë e dezinformimit dhe kërcënimet hibride.
2. Simulimet teknike dhe skenarët – Qendra organizon seanca trajnimi për qeveritë, mediat dhe agjencitë e sigurisë, në mënyrë që t'i përgatisë për sulme të mundshme informative.
3. Ngritja e kapaciteteve strategjike - mbështetja e vendeve në zhvillimin e strategjive kombëtare për mbrojtje hibride, duke përfshirë masat për parandalimin e NHMI-së.

Mësimet kryesore për Maqedoninë e Veriut në lidhje me Qendrën e Ekselencës për Kërcënimet Hibride janë:

- zhvillimi i qendrës kombëtare për kërcënimet hibride, e cila do të analizojë ndërhyrjen e huaj dhe manipulimin me informacionet në një kontekst më të gjerë;

- organizimi i ushtrimeve për institucionet bazuar në skenarë të mundshëm, në përgatitje për sulme informative; dhe
- rritjen e bashkëpunimit rajonal me NATO-n dhe BE-në, në fushën e mbrojtjes hibride.

5.2.3. SISTEMI PËR ALARMIM TË SHPEJTË E BE-SË (RAPID ALERT SYSTEM): PËRGJIGJE E SHPEJTË NDAJ KËRCËNIMEVE INFORMATIVE

Në vitin 2019, BE krijoi Sistemin për Alarmim të Shpejtë të BE-së (Rapid Alert System - RAS) si pjesë e një strategjie për mbrojtje kundër ndërhyrjes së huaj në zgjedhjet dhe proceset politike. Ky sistem mundëson shkëmbimin e shpejtë të informacionit midis Shteteve Anëtare, me qëllim identifikimin dhe kufizimin e fushatave të dezinformimit në kohë reale.

Sistemi funksionon si më poshtë:

- Shtetet Anëtare shkëmbejnë menjëherë të dhëna për operacionet e identifikuara të dezinformimit;
- Mjetet e avancuara digjitale përdoren për të monitoruar rrjetet sociale dhe faqet që përhapin dezinformim;
- Informacionet ndahen me platforma si Facebook, X dhe YouTube, të cilat kanë detyrimin të veprojnë sipas konkluzioneve të Sistemit për Alarmim të Shpejtë të BE-së (RAS).

Disa nga praktikat e mira që mund të zbatohen në Maqedoninë e Veriut janë:

- përcaktimi i mekanizmit ndërinstitucional për shkëmbimin e shpejtë të informacionit për ndërhyrjen e huaj dhe manipulimin me informacionin;
- forcimi i bashkëpunimit me platformat globale për të zvogëluar ndikimin e dezinformimit në hapësirën online; dhe
- zhvillimi i një sistemi lokal monitorimi që do të sigurojë paralajmërim të hershëm të fushatave të mundshme të dezinformimit.

REKOMANDIME PËR KRIJIMIN E POLITIKAVE PËR TRAJTIMIN E NDËRHYRJEVE TË HUAJA DHE MANIPULIMIN ME INFORMACIONET NË MAQEDONINË E VERIUT

Për të trajtuar në mënyrë efektive ndërhyrjet e huaja dhe manipulimin me informacionet, nevojitet një qasje holistike që do të adresojë aspektet institucionale, rregullatore dhe shoqërore të këtij kërcënimi. Rekomandimet e mëposhtme për krijimin e politikave kanë për qëllim forcimin e rezistencës kombëtare dhe zvogëlimin e ndikimit të dezinformimit mbi sigurinë, hapësirën mediatike dhe diskursin publik.

1. FUQIZIMI INSTITUCIONAL DHE KOORDINIMI

- Krijimi i një Qendre kombëtare për monitorimin dhe analizimin e ndërhyrjes së huaj dhe manipulimit të informacionit, e cila do të bashkojë përpjekjet institucionale për monitorimin, hetimin dhe reagimin ndaj operacioneve të huaja të dezinformimit.

- Formimi i një grupi pune ndërinstitucional me përfaqësues nga Qeveria, shërbimet e sigurisë, rregullatorët mediatik dhe sektori civil për shkëmbimin e rregullt të informacionit dhe praktikave më të mira.

- Përmirësimi i mekanizmave për komunikim të krizave, veçanërisht në rastet e rritjes së fushatave të dezinformimit në lidhje me zgjedhjet, sigurinë kombëtare ose çështjet shëndetësore dhe sociale.

- Rritja e kapaciteteve të institucioneve të sigurisë për analizën e inteligjencës së dezinformimit dhe zhvillimin e mjeteve për zbulimin e fushatave të organizuara.

- Depolitizimi i administratës publike dhe sektorit të sigurisë dhe forcimi i integritetit në menaxhimin e organeve shtetërore dhe organeve administrative përmes një qasjeje profesionale, të përgjegjshme dhe transparente në përputhje me parimet demokratike të qeverisjes

2. MASAT LEGJISLATIVE DHE RREGULLATORE

- Rishikimi i kornizave ligjore ekzistuese për dezinformimin, me përcaktim të qartë të kufirit midis lirisë së shprehjes dhe manipulimit të dëmshëm me informacionet.
- Forcimi i mbikëqyrjes së platformave online përmes rritjes së transparencës së financimit dhe reklamimit politik.
- Detyrimi për të identifikuar burimet e financimit të mediave, me qëllim parandalimin e ndikimeve të huaja përmes pronësisë së online mediave ose rrjeteve të fshehta të dezinformimit.
- Integrimi i rekomandimeve evropiane dhe të NATO-s për luftë kundër dezinformatave në rregulloren kombëtare, përafrimi me Planin e Veprimit të BE-së kundër dezinformatave dhe përmirësimi i mekanizmave të llogaridhënies.

3. FORCIMI I QËNDRUESHMËRISË DHE TRANSPARENCËS SË MEDIAS

- Mbështetje për zhvillimin e qendrave të pavarura për kontrollin e fakteve që do të bashkëpunojnë me mediat dhe do të kenë një rol zyrtar në ekspozimin e fushatave të dezinformimit.
- Rritja e transparencës në punën e medias, nëpërmjet detyrimeve për zbulimin e pronësisë dhe mbikëqyrjen e financimit të platformave online.
- Promovimi i shërbimit publik dhe mediave të pavarura përmes promovimit të gazetarisë profesionale dhe luftës kundër përhapjes së dezinformatave.

4. NDËRTIMI I REZISTENCËS SOCIAL DHE EDUKIMIT MEDIATIK

- Mirëmbajtja dhe promovimi i edukimit mediatik dhe informativ në sistemin arsimor përmes programeve arsimore për nxënësit dhe studentët për mendimin kritik dhe trajtimin e dezinformatave.

- Mbështetje për fushatat publike kundër dezinformimit, të cilat do të edukojnë qytetarët për teknikat e manipulimit të informacionit dhe rëndësinë e kontrollit të burimeve.

- Stimulimi i hulumtimit dhe analizës akademike për të zhvilluar strategji për të luftuar ndërhyrjen e huaj dhe manipulimin e informacionit, me theks të veçantë në kontekstin lokal dhe dobësitë specifike të Maqedonisë së Veriut.

5. RRITJA E BASHKËPUNIMIT NDËRKOMBËTAR

- Thellimi i partneritetit me NATO-n dhe BE-në përmes pjesëmarrjes në iniciativa të përbashkëta për shkëmbimin e të dhënave, analizën e inteligjencës dhe strategjitë për të luftuar ndërhyrjen e huaj dhe manipulimin e informacionit.

- Forcimi i bashkëpunimit me organizatat ndërkombëtare dhe qendrat kërkimore, siç është Qendra e Ekselencës për Komunikime Strategjike e NATO-s (StratCom CoE), Qendra e Ekselencës për Kërcënimet Hibride (Hybrid CoE) dhe Task Forca e Komunikimit Strategjik - BE Lindje (East StratCom Task Force), për të fituar qasje në mjetet dhe metodologjitë analitike.

- Zhvillimi i mekanizmave rajonalë për shkëmbimin e informacionit me vendet fqinje, pasi ndërhyrja e huaj dhe manipulimi i informacionit shpesh tejkalon kufijtë kombëtarë dhe ka implikime transnacionale.

Këto rekomandime synojnë të krijojnë një bazë më të fortë për mbrojtjen e shoqërisë maqedonase nga ndikimet e huaja manipuluese dhe dezinformimi. Përmes një qasjeje strategjike që përfshin forcimin institucional, reformat legjislative, rezistencën mediatike, edukimin publik dhe bashkëpunimin ndërkombëtar, shteti mund të zvogëlojë cenueshmërinë ndaj ndërhyrjes së huaj dhe manipulimit të informacionit dhe të forcojë kapacitetin demokratik për mbrojtje nga kërcënimet hibride.

PËRFUNDIM

Ndërhyrja e huaj dhe manipulimi me informacionet (NHMI) përbëjnë një kërcënim të rëndësishëm për sigurinë kombëtare, proceset demokratike dhe besimin e publikut në Maqedoninë e Veriut. Si shtet anëtar i NATO-s dhe kandidat për anëtarësim në BE, vendi është i ekspozuar ndaj formave të ndryshme të kërcënimeve hibride, duke përfshirë fushatat e organizuara të dezinformimit, manipulimin e mediave dhe sulmet kibernetike që synojnë të minojnë institucionet e saj, të rrisin polarizimin politik dhe të dobësojnë drejtimin e saj strategjik drejt integrimit euro-atlantik.

Ky studim identifikoi metodat kryesore të përdorura nga aktorë të ndryshëm për ndikim mbi mjedisin informativ të Maqedonisë, duke përfshirë krijimin dhe përhapjen e narrativave të rreme, keqpërdorimin e mediave digjitale dhe fushatat e koordinuara që synojnë grupe specifike sociale. Studimi thekson se ndërhyrja e huaj dhe manipulimi i informacionit prek disa sfera – sferat sociale, mediatike dhe kibernetike, dhe se ka dobësi sistematike që lejojnë që kërcënime të tilla të jenë efektive. Edukimi i pamjaftueshëm mediatik, niveli i ulët i besimit në institucione, mungesa e mekanizmave për reagim të shpejtë dhe kapacitetet e kufizuara për monitorimin dhe analizimin e hapësirave digjitale paraqesin pika kritike që shfrytëzohen në këto procese manipuluese.

Politikat ekzistuese dhe kornizat rregullatore në NATO dhe BE ofrojnë udhëzime dhe mekanizma për trajtimin e NHMI-së, por zbatimi i tyre në Maqedoninë e Veriut është ende në zhvillim dhe kërkon përmirësim të mëtejshëm. Analiza krahasuese ka treguar se disa vende të BE-së kanë krijuar modele më efektive për përballje me manipulimet e huaja informative, të cilat mund të shërbejnë si shembull i ndërtimit të një mekanizmi institucional dhe social më elastik.

Me qëllim forcimin e rezistencës kombëtare ndaj ndërhyrjes së huaj dhe manipulimit me informacionet, ky studim rekomandon një qasje shumëdimensionale që përfshin forcimin e kapaciteteve institucionale për detektimin dhe përgjigje ndaj dezinformatave, depolitizim të sektorit profesional të sigurisë dhe administratës publike, përmirësimin e rregulloreve për llogaridhënien, transparencën dhe integritetin e mediave, si dhe rritjen e ndërgjegjësimit publik përmes edukimit mediatik dhe informativ. Gjithashtu, me rëndësi të veçantë është rritja e bashkëpunimit me partnerët ndërkombëtarë, veçanërisht NATO-n dhe BE-në, me qëllim shkëmbimin e informacionit, praktikave të mira dhe kapaciteteve teknike për përballje me këtë lloj kërcënimi hibrid.

Maqedonia e Veriut përballet me një sfidë komplekse dhe dinamike kur bëhet fjalë për ndërhyrjen e huaj dhe manipulimin me informacionet, por me politikat e duhura strategjike, reformat institucionale dhe rritjen e ndërgjegjësimit publik, vendi mund të zvogëlojë ndikimin e operacioneve të huaja manipuluese dhe të ndërtojë një shoqëri demokratike më elastike. Lufta kundër dezinformatave dhe kërcënimeve hibride nuk është vetëm një çështje sigurie, por edhe një element kyç për mbrojtjen e vlerave demokratike dhe të ardhmen euroatlantike të vendit.

RRETH AUTORËVE

Prof. Dr., Metodi Haxhi-Janev është profesor i asociuar në Fakultetin Juridik në Universitetin „Goce Dellçev“ – Shtip dhe Akademinë Ushtarake „Gjeneral Mihailo Apostolski“ – Shkup, si dhe profesor i ftuar në Fakultetin e Inxhinierisë „Ira A. Fulton” në Universitetin Shtetëror të Arizonës, SHBA. Me përvojë ndërkombëtare në aktivitetet e mësimdhënies dhe konsulencës, ekspertiza e tij përfshin qeverisjen digjitale, menaxhimin e rrezikut dhe pajtueshmërisë, sigurinë kibernetike dhe krimin kibernetik, mbrojtjen e të dhënave, tregtinë elektronike dhe përdorimin e mjeteve dhe platformave teknologjike për avancimin e transparencës, llogaridhënies, efektivitetit, efikasitetit dhe qeverisjen e mirë. Haxhi-Janev është përfshirë si ekspert në iniciativa të shumta rajonale (në Evropën Juglindore, përfshirë Moldavinë dhe Gjeorgjinë) dhe organizata ndërkombëtare, të tilla si USAID, Departamenti Amerikan i Shtetit, BE, NATO, RCC (me qendër në Sarajevë) dhe RACVIAC (me qendër në Zagreb), duke u përqendruar në ngritjen e kapaciteteve, përfshirjen e palëve të interesuara dhe zbatimin e strategjive të menaxhimit, rrezikut dhe pajtueshmërisë. Puna e tij lidh sektorin publik, akademik dhe privat me qëllim nxitjen e qeverisjes së mirë, transparencës dhe inovacionit digjital. Ai është gjithashtu i përfshirë në vlerësimin e nivelit të lartë në institucione si Komisioni Evropian, Fondacioni Evropian i Shkencës dhe Agjencia Sllovake për Kërkim dhe Zhvillim, dhe kontribuon në Rrjetin Global të Vlerësimit të Sigurisë të udhëhequr nga Harvardi.

Marjan Stoilkovski është Udhëheqës i Shërbimit të Sigurisë së TI-së në NLB Banka, ndërsa më parë, për 15 vjet ishte Udhëheqës i Sektorit për Krim Kompjuterik dhe Forensikë Digjitale në Ministrinë e Punëve të Brendshme. Për më shumë se 13 vjet, ka punuar si ekspert ndërkombëtar për sigurinë kibernetike, krimin kibernetik, forenzikën digjitale dhe provat elektronike. Ka kryer më shumë se 80 aktivitete ndërkombëtare për të forcuar kapacitetet e sigurisë kibernetike dhe krimit kibernetik si pjesë e aktiviteteve të projektit të Këshillit të Evropës, Komisionit Evropian, Kombeve të Bashkuara, OSBE-së dhe institucioneve dhe organizatave të tjera ndërkombëtare. Aktualisht, fokusi i tij shkencor dhe profesional është në fushën e sigurisë kibernetike, respektivisht zbatimin e zgjidhjeve të sigurisë dhe testimit, përgatitjen dhe zbatimin e Tabletop Exercises ushtrimeve praktike, menaxhimin e incidenteve dhe forenzikës digjitale, SOC Managed services dhe malware analyses. Hulumtimet shtesë përfshijnë Virtual assets në aspektin e analizës dhe rregullimit, OSINT dhe burimet e hapura të informacionit (dhe DARKNET), dhe përdorimin e IA në aktivitetet operacionale të sigurisë kibernetike.

LITERATURA E PËRDORUR

- Shoqata e Gazetarëve të Maqedonisë (2023). Media Freedom in North Macedonia: Fragile Progress, e qasshme në: 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, në dispozicion në: https://www.bbc.co.uk/bitesize/articles/zbw492p
- BIRN Macedonia (2023). Media Ownership Monitor – North Macedonia, në dispozicion në: https://north-macedonia.mom-gmr.org/mk/
- Blue Europe (2024). Challenges of Chinese Soft Power in Western Balkans, në dispozicion në: 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, në dispozicion në: 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, në dispozicion në: https://corporatefinanceinstitute.com/resources/valuation/platform-company/
- CSIS, (2021), Reimagining U.S. Policy toward the Western Balkans, në dispozicion në: 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. në dispozicion në: https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf
- Deutche Welle (2024), “What is foreign information manipulation and interference?”, në dispozicion në: https://akademie.dw.com/en/what-is-foreign-information-manipulation-and-interference/video-68790017
- EU COMMISSION STAFF WORKING DOCUMENT, North Macedonia 2023 Report, në dispozicion në: 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, në dispozicion në: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- EU Commission, (Brussels, 8.11.2023), North Macedonia 2023 Report, Commission Staff Working Document, në dispozicion në: 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, në dispozicion në: https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
- EUEA (2025), Brenda infrastrukturës së operacioneve të manipulimit dhe ndërhyrjes së informacionit të huaj (FIMI), në dispozicion në: https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en
- European Commission. Separating facts from fiction on vaccines, në dispozicion në: 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,, në dispozicion në: https://datasociety.net/library/data-voids/
- https://www.facebook.com/photo.php?fbid=1101727971749705&id=100057375372607&set=a.285088090080368&locale=tr_TR
- Hubervic A., Prudent Y., for Enabling Alliance Interoperability and Pervasive M&S Applications. NATO Science and Technology Organisation (STO), në dispozicion në: линк
- Jakov Marusic S., (2022). Forget Sputnik. Russian Propaganda Has other Paths into North Macedonia, BIRN, në dispozicion në: 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, në dispozicion në: 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, në dispozicion në: 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, në dispozicion në: https://project-athena.eu/decoding-fimi-a-complex-interrelation-with-disinformation/
- PBS News (2017). Trump retweets anti-Muslim videos from British far-right leader, në dispozicion në 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, në dispozicion në 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, në dispozicion në: 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, në dispozicion në: 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. në dispozicion në: 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)" në dispozicion në: 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, në dispozicion në: 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, në dispozicion në: 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, në dispozicion në: 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, në dispozicion në: https://www.washingtonpost.com/news/the-fix/wp/2015/11/22/trump-retweeted-a-very-wrong-set-of-numbers-on-race-and-murder/
- Agjencia për Shërbime Audio dhe Audiovizuele (ASHMAAV). Rrjeti për edukim mediatik - https://mediumskapismenost.mk/
- Analiza e profileve aktive në mediat sociale. Për shembull, "Në rrugën drejt Maqedonisë" (11 janar 2025), në dispozicion në:
- Gazeta e Republikës së Maqedonisë së Veriut" nr. 152/2019 dhe 275/2019)
- Vërtetmatësi, (2023). Putin në Sheshin e Kuq përsëriti narracionet kryesore të dezinformimit – Rusia është viktimë dhe ka mbrojtur veten!, në dispozicion në: https://vistinomer.mk/putin-na-crveniot-ploshtad-gi-povtori-glavnite-dezinformaciski-narativi-rusija-e-zhrtva-i-se-branela/
- Qeveria e Republikës së Maqedonisë së Veriut (2024), në dispozicion në: https://ener.gov.mk/Default.aspx?item=pub_regulation&subitem=view_reg_detail&itemid=51471
- Qeveria e Republikës së Maqedonisë së Veriut, (2021), "Strategjia për ndërtimin e rezistencës kombëtare dhe ballafaqimin me kërcënimet hibride", në dispozicion në: https://mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf
- Komisioni Evropian, Dokumenti i Punës së shërbimeve të komisionit, Raporti për Maqedoninë e Veriut për vitin 2021, Strasburg, 19.10.2021, Kuvendi i Republikës së Maqedonisë së Veriut
- EEA (2023). „Beyond Disinformation - What is FIMI?", në dispozicion në: https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en#:~:text=Tackling%20Disinformation%2C%20Foreign%20Information%20Manipulation,democratic%20processes%2C%20security%20and%20citizens

- Ligji për komunikimet elektronike (“Gazeta zyrtare e Republikës së Maqedonisë” nr. 39/2014), 188/2014, 44/2015, 193/2015, 11/2018 dhe 21/2018 dhe “Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 98/2019 dhe 153/2019

- Ligji për mbrojtjen e të dhënave personale (Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 42/20)

- Ligji për ndryshimin dhe plotësimin e Ligjit për Mbrojtjen e të Dhënave Personale (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut nr. 294/21)

- Ligji për Procedurën Penale (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut”, nr. 150/10, 100/12, 142/16 dhe 198/18)

- Ligji për të Drejtën e Fëmijëve (“Gazeta Zyrtare e Republikës së Maqedonisë nr. 148/2013 dhe “Gazeta

- Ligji për ndjekjen e komunikimeve (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr.71/18)

- Ligji për shërbime mediatike audio dhe audiovizuele (tekst i konsoliduar) (Gazeta Zyrtare nr. 184/2013, Gazeta Zyrtare nr. 13/2014 dhe Gazeta Zyrtare nr. 44/2014), në dispozicion në: Zakon-za-Audio-i-audiovizuelni-mediumski-uslugi-prechisten-tekst-na-memorandum.pdf

- Ligji për mbrojtjen e fëmijëve “Gazeta Zyrtare e Republikës së Maqedonisë” nr. 23/2013, 12/2014, 44/2014, 144/2014, 10/2015, 25/2015, 150/2015, 192/2015, 27/2016, 163/2017, 21/2018 dhe 198/2018 dhe Gazeta Zyrtare e Republikës së Maqedonisë së Veriut, nr. 104/2019, 146/2019, 275/2019, 311/2020 dhe 294/2021)

- Instituti për Studime të Komunikimit (2023). Cenueshmëria ndaj dezinformatave në mesin e grupeve të ndryshme të qytetarëve në Maqedoninë e Veriut. Res publika, në dispozicion në: https://iks.edu.mk/istrazuvanja-analizi/ranlivost-na-dezinformacii-kaj-razlichni-grupi-gragjani-vo-severna-makedonija/

- Instituti për Studime të Komunikimit (2024). Praktikat dhe perceptimet e qytetarëve në drejtim të informimit dhe trajtimit të dezinformatave. Res publika, në dispozicion në: https://iks.edu.mk/istrazuvanja-analizi/praktiki-i-percepcii-na-gragjanite-vo-pogled-na-informiranjeto-i-spravuvanjeto-so-dezinformaciite/

- Jakimova J., (2022), „Kur nuk ka besim në shtet -grumbullohet vaji dhe vaksinat refuzohen“, Radio Evropa e Lirë, në dispozicion në: link

- Klinçarski P., Gaxhovska Spasovska Z. (2024), Paratë shtetërore për OJQ-të në duart e disa prej administratorëve të BDI-së, Radio Evropa e Lirë, në dispozicion në: https://www.slobodnaevropa.mk/a/drzhavni-pari-za-nevladini-vo-racete-na-del-od-administrativcite-na-dui/32788912.html

- Kodi penal (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr. 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 dhe numër 36/23

- MIA, (9 prill 2022), “Petrovska: Asnjë strategji e kërcënimit hibrid nuk mund të zbatohet plotësisht nëse nuk marrin pjesë të gjithë aktorët në vend,” në dispozicion në link

- Ministria e Mbrojtjes (2020). Strategjia për mbrojtje kibernetike, në dispozicion në: https://mod.gov.mk/inc/uploads/2021/06/Strategija-za-sajber-odbrana-mk-1-1.pdf

- Micevski I., Trpevska S. (2024). Monitorimi i pluralizmit mediatik në epokën digjitale - Zbatimi i monitorimit të pluralizmit mediatik në shtetet anëtare të BE-së dhe vendet kandidate në vitin 2023 - Raporti Kombëtar: Republika e Maqedonisë së Veriut. Instituti për kërkime për zhvillim social – RESIS, në dispozicion në: https://cadmus.eui.eu/bitstream/handle/77022/1814/North_Macedonia_MK_mpm_2024_cmpf.pdf?sequence=2&isAllowed=y

- Pavlovska J. (2024). Në spiralen e krimit: Pak përvetësim, pak korrupsion dhe gjithçka nga e para dhe përsëri, Nova Makedonija, në dispozicion në: https://novamakedonija.com.mk/pecateno-izdanie/vo-spiralata-na-kriminalot-red-pronevera-red-korupcija-i-s%D-90%1odnovo-i-povtorno/

- Pfeiffer H. (2024). Rrjeti i ekspozuar i propagandës ruse në Evropë, Deutsche Welle, në dispozicion në: https://www.dw.com/mk/razotkriena-mreza-za-ruska-propaganda-vo-evropa/a68698125-

Институт за комуникациски студии

НЕ ВЕРУВАЈ ПРОВЕРУВАЈ! #користифакти

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

British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

Ky produkt është përgatitur në kuadër të projektit „Përdorimi i gazetarisë së bazuar në fakte për rritjen e ndërgjegjësimit dhe për luftë kundër dezinformatave në hapësirën mediatike në Maqedoninë e Veriut“ financuar nga Qeveria e Mbretërisë së Bashkuar, me mbështetjen e Ambasadës Britanike në Shkup. Mendimet dhe qëndrimet e shprehura në këtë përmbajtje nuk pasqyrojnë çdo herë mendimet dhe qëndrimet e Qeverisë Britanike.

Институт за комуникациски студии

НЕ ВЕРУВАЈ ПРОВЕРУВАЈ! #користифакти