

REAGIMI INSTITUCIONAL NDAJ NDËRHYRJES SË HUAJ DHE MANIPULIMIT ME INFORMACIONET NË MAQEDONINË E VERIUT: MODELET DHE OPSIONET PËR POLITIKA

DOKUMENT PËR POLITIKA PUBLIKE

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

Rreth botuesit:
prof. dr. Zaneta Trajkoska

Edicioni:
ResPublica

Autorë:
dr. Aleksandar Grizhev, profesor i asociuar
dr. Vesna Poposka, profesoreshë e asociuar

Redaktor:
mr. Dejan Andonov

Përkthim nga maqedonisht në shqip:
Vjosa Taipi

Titulli origjinal:
„Институционален одговор на странско мешање и манипулирање со информации во Северна Македонија: модели и опции за политика" - документ за јавна политика

Dizajni grafik:
Ivana Temelkoska

Vendi dhe viti:
Shkup, 2025

PËRMBAJTJA

REZYME 5

HYRJE 7

Metodologjia 9

1. Korniza dhe qasja metodologjike 9

2. Burimet e të dhënave 9

3. Mostra dhe pjesëmarrësit 10

4. Etika 10

5. Kufizimet 11

KAPITULLI 1: DREJT NJË PËRGJIGJEJE TË INTEGRUAR NDAJ KËRCËNIMEVE TË INFORMACIONIT 12

1.1. Kërcënimet e informacionit dhe nevoja për një përgjigje të koordinuar institucionale 13

1.2. Ndërhyrja në zgjedhje ndër operacionet më komplekse të NHMI-së 15

1.3. Qasja e përgjegjshme dhe analitike e BE-së ndaj NHMI-së 18

KAPITULLI 2: SITUATA DHE SFIDAT E REAGIMIT INSTITUCIONAL NDAJ NHMI-SË NË MAQEDONINË E VERIUT 23

2.1. Gjetjet e sintetizuara nga hulumtimi cilësor 24

2.1.1. Konsiderata dhe perceptime të përgjithshme 24

2.1.2. Organizimi dhe koordinimi institucional 25

2.1.3. Kuadri legjislativ dhe strategjik 26

2.1.4. Kapacitetet dhe burimet 26

2.1.5. Perceptimi i mundësive dhe sugjerime për përmirësim 27

2.1.6. Sfidat kryesore 27

2.2. Analiza e statusit të sistemit (GAP Analysis) 28

2.2.1. Organizimi dhe koordinimi institucional 29

2.2.2. Kuadri strategjik (operacionalizimi) 30

2.2.3. Kapacitetet dhe burimet 30
2.2.4. Standardet për shkëmbimin e informacioneve 31
2.2.5. Qëndrueshmëria e komunikimit dhe edukimi 31
2.2.6. Monitorimi dhe vlerësimi 31

KAPITULLI 3: PËRVOJAT KRAHASUESE DHE MODELET E REAGIMIT NDAJ NHMI 32

3.1. Estonia: një shtet digjital me rutina ndërgjegjësimi dhe koordinimi 35
3.2. Franca (Viginum): kapaciteti kryesor i qeverisë kundër ndërhyrjeve digjitale 36
3.3. Polonia: vlerësimi ndër-sektorial i rrezikut dhe informimet tremujore 36
3.4. Suedi: Agjencia për Mbrojtje Psikologjike 37
3.5. Finlanda: edukimi, partneritete dhe komunikime parandaluese 38

KAPITULLI 4: OPSIONET PËR POLITIKËN E REAGIMIT NDAJ NHMI-SË NË MAQEDONINË E VERIUT 39

4.1. Opsioni A: Qendra e Pavarur Kombëtare për Qëndrueshmëri 40
4.2. Opsioni B: Mekanizmi Kombëtar i Koordinimit në kuadër të Qeverisë 41
4.3. Opsioni C: Forcimi i Këshillit ekzistues për Koordinim të Komunitetit të Inteligjencës së Sigurisë 43

KAPITULLI 5: PËRFUNDIM DHE REKOMANDIME PËR ZBATIM 47

5.1. Vërejtje përfundimtare 48
5.2. Rekomandime për zbatimin 49

PËR AUTORËT 52

LITERATURA E PËRDORUR 53

REZYME

Në Maqedoninë e Veriut, ekziston vetëdija për rreziqet që vijnë nga ndërhyrja e huaj dhe manipulimi me informacionin (NHMI), por sistemi i reagimit të koordinuar në vend mbetet i fragmentuar, pa koordinim funksional ndërinstitucional dhe kompetenca të përcaktuara qartë. Mungesa e një mekanizmi të centralizuar për shkëmbimin e informacionit, analizën në kohë dhe reagimin e përbashkët. Shumica e aktiviteteve kryhen në mënyrë reaktive, në varësi të iniciativës së institucioneve ose sektorëve individualë, gjë që mund të çojë në kompetenca të mbivendosura, humbje të burimeve dhe komunikim të gabuar me publikun.

Kapacitetet dhe burimet e kufizuara, të tilla si stafi, mjetet dhe buxhetet për monitorimin, analizën dhe komunikimin strategjik, dhe mungesa e edukimit sistematik të sektorit publik në fushën e edukimit digjital dhe mediatik e bëjnë të vështirë luftimin e NHMI-së. Kjo plotësohet nga niveli i ulët i besimit të publikut (IRI, 2024) dhe qëndrueshmërisë sociale, i nxitur nga polarizimi dhe transparenca e pamjaftueshme e komunikimit institucional.

Ndërhyrja e huaj dhe manipulimi i informacionit nuk është përcaktuar qartë në kuadrin rregullator dhe strategjitë ekzistuese nuk janë funksionalizuar mjaftueshëm përmes roleve, protokolleve dhe treguesve të qartë për të monitoruar dhe matur suksesin e tyre. Këshilli Koordinues i Komunitetit të Inteligjencës së Sigurisë nuk kryen funksionet e synuara, dhe në praktikë nuk ka strukturë të krijuar për analizë të shpejtë dhe reagim të përbashkët në rastet e dezinformimit ose ndikimit të huaj.

Prandaj, rekomandimi kryesor i këtij dokumenti për politika publike është që Maqedonia e Veriut duhet të krijojë një mekanizëm kombëtar për koordinimin dhe qëndrueshmërinë e NHMI-së, i cili do të sigurojë lidhjen institucionale, shkëmbimin e rregulluar të informacionit dhe monitorimin sistematik të kërcënimeve me role të qarta, protokolle dhe tregues të performancës.

Dokumenti ofron opsionet e mëposhtme të zgjidhjes institucionale:

- Krijimi i një qendre të pavarur për qëndrueshmëri digjitale ose kombëtare - nënkupton krijimin e një institucioni të pavarur publik me mandat, përgjegjësi dhe buxhet të qartë, i cili do të integronte funksionet e analizës, koordinimit dhe edukimit. Avantazhi është në strukturën e centralizuar dhe të dukshme, por modeli kërkon burime të reja dhe konfigurim administrativ.

- Krijimi i një mekanizmi kombëtar të koordinimit në kuadër të Qeverisë - parashikon integrimin e mekanizmit përmes një zyre koordinimi "bërthamë + rrjet". Kjo do të sigurojë peshë politike, ndërveprim dhe reagim të shpejtë në situata krize, por një rrezik i mundshëm është mbingarkesa me çështje të tjera, varësia nga vazhdimësia politike dhe mungesa e mundshme e analizave të thella nëse bërthama është e vogël.

- Integrimi në Këshillin Koordinues të Komunitetit të Inteligjencës dhe Sigurisë - mundëson forcimin dhe funksionalizimin e një strukture ekzistuese duke zgjeruar mandatin

e saj në fushën e NHMI-së. Avantazhi është në racionalizimin e një strukture tashmë të krijuar, por rreziku është në shikueshmërinë dhe koordinimin më të ulët të publikut për të mbetur "në letër", gjë që kërkon disiplinë dhe procedura të qarta të funksionimit të standardeve.

Pavarësisht nga opsioni që do të zgjidhej, ky dokument propozon **rekomandimet e mëposhtme për krijimin e një sistemi të qëndrueshëm dhe funksional për trajtimin e NHMI-së**:

- Përcaktimi i një modeli institucional dhe transportuesi dhe emërtimi i pikave të kontaktit në të gjitha institucionet përkatëse;
- Vendosja e një kalendari të rregullt të aktiviteteve, hartimi i një procedure standarde "raport – vlerësim - reagim" për menaxhimin e incidenteve dhe zhvillimi i skenarëve universalë dhe listave për kontroll;
- Forcimi i kapaciteteve njerëzore;
- Komunikimi parandalues rreth narrativave manipuluese të pritshme;
- Shkëmbimi i informacionit përmes një baze të përbashkët; dhe
- Krijimi i treguesve për monitorimin e performancës.

Ekziston gjithashtu nevoja që institucionet të marrin masa dhe politika shtesë që do të forcojnë sistemin dhe qëndrueshmërinë e tij, siç janë:

- Rishikimi dhe azhurnimi i Strategjisë ekzistuese për Rezistencën ndaj Kërcënimeve Hibride (2021–2025);
- Forcimi i kapaciteteve institucionale për monitorim dhe analizë;
- Prezantimi i programeve për edukim mediatik dhe digjital në sektorin publik;
- Përfshirja e sektorëve akademikë dhe qytetarë përmes partneriteteve të formalizuara; dhe
- Integrim më i madh me mekanizmat e NATO-s dhe BE-së për të luftuar NHMI-në.

Krijimi i një modeli kombëtar për trajtimin e NHMI-së do t'i mundësojë Maqedonisë së Veriut të lëvizë drejt një sistemi të integruar, funksional dhe të qëndrueshëm të reagimit institucional.

HYRJE

Në kontekstin modern të sigurisë dhe informacionit, manipulimi i huaj dhe ndërhyrja në informacion (NHMI) përbën një kërcënim serioz dhe në rritje për sistemet demokratike, besimin e publikut dhe stabilitetin e institucioneve. Zhvillimi i shpejtë i teknologjive digjitale, lidhja në rritje dhe natyra transnacionale e flukseve të informacionit lejojnë që operacione të tilla të kryhen në mënyrë më efikase dhe më të vështirë për tu zbuluar. Përmes përdorimit të rrjeteve të koordinuara, identiteteve të fshehta dhe inteligjencës artificiale gjeneruese, aktorët shtetërorë dhe jo shtetërorë mund të ndikojnë në opinionin publik, proceset zgjedhore dhe politikën e jashtme të vendeve të tjera. Në një kontekst evropian, NHMI-ja njihet si një kërcënim i sigurisë dhe politikës së jashtme që kërkon një përgjigje të koordinuar, ndër-sektoriale, me theks jo vetëm në përmbajtje, por edhe në taktikat, teknikat dhe procedurat e ndikimit dhe ndërhyrjes. Institucionet evropiane tashmë kanë aktivizuar mekanizma të koordinuara për rritjen e gatishmërisë në periudhat zgjedhore, gjë që thekson rëndësinë e masave proaktive, jo vetëm reaktive.

Në Maqedoninë e Veriut, NHMI-ja po fiton gjithnjë e më shumë rëndësi në kontekstin e integrimit euro-atlantik dhe nevojës për të forcuar rezistencën kombëtare ndaj kërcënimeve hibride. Ekziston një konsensus në vend për rëndësinë e fenomenit në kuadër të politikave kombëtare për kërcënimet hibride dhe integritetin zgjedhor, të forcuara nga miratimi i Strategjisë Kombëtare për Ndërtimin e Rezistencës dhe Ballafaqimin me Kërcënimet Hibride (2021–2025) dhe Plani i Veprimit shoqërues. Siç shkruhet në strategjinë, qëndrueshmëria bazohet në një orientim strategjik drejt një qasjeje të integruar, më të koordinuar dhe ngritjes së kapaciteteve në nivel kombëtar, në përputhje me detyrimet e gatishmërisë civile të NATO-s dhe nevojat kombëtare të qëndrueshmërisë. Megjithatë, operacionalizimi i strategjisë dhe planit të veprimit mbetet një sfidë për institucionet, nuk ka inkriminim të fenomeneve të tilla dhe reagimi institucional përballet me koordinim të pamjaftueshëm, burime të kufizuara njerëzore dhe teknike, shpërndarje të paqartë të kompetencave dhe mungesë monitorimi, analize dhe përgjigje sistematike ndaj rreziqeve.

Në sistemin ligjor maqedonas, nuk ka përkufizim të miratuar në mënyrë eksplicite për manipulimin e huaj dhe ndërhyrjes në informacion, gjë që kontribuon që problemi të mbetet pjesërisht i keqkuptuar dhe i trajtuar në mënyrë joadekuate në politikat publike. Nga këndvështrimi i politikave dhe rregulloreve të BE-së, termi gjithashtu përfshin përmbajtjen dhe sjelljet - në shumë raste, NHMI-ja është një formë e dezinformimit me origjinë të huaj, por gjithashtu përfshin taktika dhe procedura operacionale, të tilla si sjellje të koordinuara jo autentike, shkelje teknike, rrjedhje materiale dhe operacione hibride, që synojnë formimin dhe shprehjen e lirë të vullnetit politik (Blair-Simon K., 2025).

Kjo spirancë e dyfishtë - korniza kombëtare për kërcënimet hibride dhe korniza evropiane për integritetin e mjedisit të informacionit, e udhëheq edhe këtë dokument, përkatësisht përkufizimi i përdorur është operativ (bazuar në sjelljet dhe proceset) dhe ka për qëllim parandalimin, zbulimin dhe reagimin e koordinuar.

Ky dokument politikash synon të lokalizojë dhe analizojë problemin e koordinimit ndërinstitucional për ballafaqim me NHMI-në, si dhe të propozojë zgjidhje konkrete dhe të realizueshme për krijimin e sistemit kombëtar të reagimit, si pjesë e përpjekjeve më të gjera për të ndërtuar qëndrueshmëri institucionale dhe sociale ndaj kërcënimeve hibride. Fokusi është në modelet organizative, mekanizmat e koordinimit dhe instrumentet e monitorimit dhe reagimit. Kjo qasje e kombinuar bën të mundur lidhjen e narrativëve dhe proceseve, përkatësisht si ndodh ndikimi, me kapacitetet institucionale, pra si të menaxhohet rreziku me rekomandimet e zbatueshme.

Dokumenti bazohet në kuadrin ekzistues evropian dhe kombëtar, duke përfshirë detyrimet që rrjedhin nga anëtarësimi në NATO dhe procesi i përafrimit me BE-në. NATO forcon rolin e komunikimit strategjik përmes Qendrës së Ekselencës në Riga (*StratCom - NATO Strategic Communications Centre of Excellence*) në mbështetje të vendeve aleate dhe partnere në ndërtimin e kapaciteteve për analiza, komunikim dhe parandalim, ndërsa Sistemi për alarmin të shpejtë (*Rapid Alert System – RAS*) shërben për të koordinuar dhe shkëmbyer informacion midis shteteve anëtare në incidentet informative. Paralelisht, BE përcakton detyrime sistematike për menaxhimin e rrezikut, duke përfshirë dezinformimin, për platformat e mëdha online përmes Aktit për Shërbime Digjitale (*DSA*) dhe përcakton standarde për pavarësinë dhe pluralizmin e medias përmes Aktit Evropian për Lirinë e Medias (*EMFA*). Së fundi, dokumenti bazohet në dy studimet e mëparshme të Institutit për Studime të Komunikimit: Ndërhyrja e huaj dhe manipulimi i informacionit në Republikën e Maqedonisë së Veriut: një analizë dalëse (Haxhi-Janev M., Stoillkovski M.,2025) dhe duke iu referuar ndërhyrjes së huaj dhe manipulimit të informacionit në kontekstin e rregulloreve evropiane (Blair-Simon K.,2025).

Dokumenti përshkruan situatën aktuale ("ku jemi") në strukturën institucionale, kapacitetet dhe kuadrin rregullator, identifikon boshllëqet thelbësore midis synimeve strategjike dhe praktikës aktuale, ofron opsione të politikave (modele alternative institucionale) bazuar në përvojat krahasuese dhe propozon një udhërrëfyes për zbatim. Prandaj, është strukturuar në seksionet e mëposhtme:

Kapitulli 1: Drejt një përgjigjeje të integruar ndaj kërcënimeve të informacionit;

Kapitulli 2: Situata dhe sfidat e reagimit institucional ndaj NHMI-së në Maqedoninë e Veriut;

Kapitulli 3: Përvojat krahasuese dhe modelet e reagimit ndaj NHMI;

Kapitulli 4: opsionet për politikën e reagimit ndaj NHMI-së në Maqedoninë e Veriut; dhe

Kapitulli 5: Përfundim dhe rekomandime për zbatim.

Me këtë strukturë, dokumenti u mundëson vendimmarrësve, ekspertëve dhe publikut të gjerë të perceptojnë kufizimet aktuale institucionale dhe të njohin drejtimet konkrete për zhvillimin e një sistemi të integruar, proaktiv dhe të koordinuar të rezistencës ndaj ndërhyrjes së huaj dhe manipulimit të informacionit.

Metodologjia

1. Korniza dhe qasja metodologjike

Analiza bazohet në një qasje të kombinuar metodologjike që lidh (1) një desk analizë të politikave dhe dokumenteve përkatëse kombëtare të BE-së dhe NATO-s (2) gjetjet cilësore nga grupet e fokusit dhe intervistat me përfaqësues nga institucionet kryesore; (3) analizë të situatës (*GAP analysis*) të sistemit institucional; dhe (4) analizë krahasuese të praktikave të mira nga vendet anëtare të BE-së dhe NATO-s (Estonia, Finlanda, Franca, Polonia dhe Suedia). Qëllimi është të arrihet një pamje e integruar: (a) se si NHMI-ja manifestohet dhe perceptohet në praktikë; (b) deri në çfarë mase kuadri dhe kapacitetet institucionale mundësojnë një përgjigje efektive; dhe (c) cilat modele janë të zbatueshme në Maqedoninë e Veriut. Rezultatet e analizës shërbejnë si bazë për zhvillimin e rekomandimeve të politikave, të cilat do të mundësojnë ndërtimin e një sistemi më gjithëpërfshirës dhe më të integruar për parandalimin dhe menaxhimin e rreziqeve të NHMI-së.

2. Burimet e të dhënave

(a) Desk analizë. Rregulloret dhe politikat përkatëse të BE-së dhe NATO-s (Akti i Shërbimeve Digjitale - *DSA*; Akti Evropian për Lirinë e Medias - *EMFA*; Koncepti Strategjik i NATO-s (2022); Seti i mjeteve për përgjigje ndaj NHMI (*FIMI Toolbox*), Sistemi për Alarm të Shpejtë (*Rapid Alert System - RAS*), etj.), Strategjia Kombëtare për Ndërtimin e Rezistencës dhe Kundërshtimin e Kërcënimeve Hibride (2021–2025) me Planin e Veprimit, si dhe botimet e mëparshme të IKS u shqyrtuan për të siguruar kontekstin normativ-politik. Rezultatet e desk analizës janë trianguluar me gjetjet e grupeve të fokusit për të ndërtuar një interpretim koherent të boshllëqeve sistemike ndërsa duke kombinuar burimet dhe teknikat, vlefshmëria e gjetjeve mund të rritet (Bryman, 2016). Në hartimin e monitorimit dhe vlerësimit u udhëhoqëm nga udhëzimet e Organizatës për Bashkëpunim dhe Zhvillim Ekonomik (*OECD*) për monitorimin dhe vlerësimin e politikave publike (OECD, 2017).

(b) Grupet e fokusit. Dy grupe fokusi u zhvilluan me përfaqësues nga institucionet kryesore dhe rregullatorët në shtator 2025. Diskutimet ishin gjysmë të strukturuara sipas një udhëzuesi me pesë objektiva tematike: kuptimi i NHMI-së, koordinimi institucional, kuadri ligjor ose strategjik, kapacitetet dhe burimet, si dhe bashkëpunimi ndërkombëtar. Seancat u mbajtën në një mjedis të kontrolluar (90-120 minuta), me moderim nga një ekip kërkimor, ndërsa të dhënat u mbajtën si shënime dhe transkriptime. Të anketuarit që nuk mund të merrnin pjesë në grupet e fokusit iu përgjigjën një pyetësori për intervista. Deklaratat në dokument janë parafrazuar për të ilustruar tendencat e përsëritura

dhe gjetjet janë paraqitur si një pasqyrë e perceptimeve të zakonshme dhe sfidave sistematike, në mënyrë që të nxirren pika analitike në lidhje me nivelin aktual të pjekurisë dhe qëndrueshmërisë institucionale.

(c) Analiza e situatës (*GAP analysis*). U bë një krahasim midis synimeve dhe detyrimeve strategjike dhe praktikës reale institucionale në aspektin e roleve dhe kompetencave, proceseve të koordinimit dhe shkëmbimit të informacionit, personelit dhe burimeve teknike dhe mekanizmave të monitorimit dhe vlerësimit. Boshllëqet janë përmbledhur sipas domenit dhe përdoren si një urë lidhëse për opsionet politike dhe udhërrëfyesin për zbatim.

(d) Analiza krahasuese. Pesë modele referimi nga vendet anëtare të BE-së dhe NATO-s (Estonia, Finlanda, Franca, Polonia dhe Suedia) u zgjodhën sipas kritereve të mëposhtme të zbatueshmërisë: mandati dhe proceset e përcaktuara qartë, koordinimi ndër-sektorial, mjetet dhe stafi, komunikimi strategjik transparent dhe rezultatet e matshme.

3. Mostra dhe pjesëmarrësit

Hulumtimi cilësor përdori "mostër të qëllimshme" *(purposive sampling*), ku relevanca e pjesëmarrësit për objektivin e hulumtimit ka përparësi mbi përfaqësueshmërinë statistikore (Bryman, 2016). Mostra mbuloi nivelet e ndryshme të administratës publike (strategjike, operacionale dhe analitike), në mënyrë që të sigurojë një vështrim shumë shtresor në proceset e planifikimit, zbatimit dhe vlerësimit. Përfaqësimi i përfaqësuesve nga strukturat e koordinimit të qeverisë, sektorët e sigurisë dhe inteligjencës, portofoli diplomatik-konsullor dhe nga resorët për transformim digjital, administratë publike, TIK- siguria dhe rregullimi i mediave, bëri të mundur krahasimin e perspektivave institucionale (normative dhe organizative) me përvojat operacionale (procedurat reale, pengesat, kufizimet). Hulumtimi përfshiu institucionet e mëposhtme: Ministritë e Punëve të Jashtme, Punëve të Brendshme, të Transformimit Digjital dhe Administratës Publike, Komitetin Kombëtar për Parandalimin e Ekstremizmit të Dhunshëm dhe Luftë Kundër Terrorizmit, Agjencinë e Inteligjencës (AZ), Agjencinë për Shërbime Mediatike Audio dhe Audiovizive (AShMAA), Qendrën Kombëtare për Incidenteve Kibernetike (MKD-CIRT), Qendrën për Menaxhim me Kriza dhe Drejtorinë për Prodhim të Synuar në Ministrinë e Ekonomisë.

4. Etika

Duke pasur parasysh ndjeshmërinë e temës, veçanërisht për institucionet me kompetenca të sigurisë, hulumtimi u krye sipas protokolleve të qarta etike. Të gjithë pjesëmarrësit u informuan për qëllimin, mënyrën e përdorimit të të dhënave dhe masat e mbrojtjes së identitetit. Raporti nuk specifikon emra, detyra ose institucione specifike për të ruajtur konfidencialitetin dhe për të shmangur atribuimin e nënkuptuar të pikëpamjeve ndaj një institucioni të caktuar. Segmentet që mund t'i referohen praktikave specifike operacionale

grumbullohen në nivel tematik dhe konkluzionet formulohen si një sintezë e tendencave të përsëritura, jo si pretendime individuale. Në këtë mënyrë zvogëlohen rreziqet e keqinterpretimit dhe ruhet konfidencialiteti pa kompromentuar vlerën analitike.

5. Kufizimet

Në mënyrë tipike për studime cilësore, grupet e fokusit nuk pretendojnë përfaqësim, por sigurojnë një kuptim të thellë të proceseve dhe perceptimeve. Përdorimi i citateve të parafrazuara zvogëlon mundësinë e citimit të fjalëpërfjalshëm, por në të njëjtën kohë bën të mundur ruajtjen e thelbit të argumentimit. Anshmëria e mundshme e sjelljes së dëshirueshme shoqërore u zbut përmes teknikave të moderatorit (shkelja e pyetjeve, kërkimi i shembujve konkretë, synimi i proceseve në vend të qëndrimeve personale) dhe përmes triangulimit të dokumenteve dhe përvojave krahasuese. Pretendimet përfundimtare në dokument bazohen në konvergjencën midis burimeve të shumëfishta dhe jo deklaratave të vetme (Bryman, 2016).



KAPITULLI 1:

DREJT NJË PËRGJIGJEJE TË INTEGRUAR NDAJ KËRCËNIMEVE TË INFORMACIONIT

1.1. Kërcënimet e informacionit dhe nevoja për një përgjigje të koordinuar institucionale

Ndërhyrja e huaj dhe manipulimi i informacionit (NHMI) mbulon spektrin e përmbajtjes dhe, më e rëndësishmja, praktikat e sjelljes me të cilat aktorët e huaj përpiqen të prishin ose drejtojnë debatin publik, të ndikojnë në proceset demokratike dhe të dëmtojnë besimin në institucione. Në qasjen evropiane, SMMI-ja nuk trajtohet vetëm si "përmbajtje e dëmshme", por edhe si taktika, teknika dhe procedura (*TTPs*), të tilla si hakimi dhe publikimi (*hack-and-rrjedhje*), informacion i rremë i kompjuterizuar, aktivitete të koordinuara jo autentike, etj. (Blair-Simon K., 2025). Në literaturë, kjo përshkruhet më tej si operacione kognitive dhe ndikim algoritmik në sferën publike (Pamment, 2020). Masat moderne aktive funksionojnë si fushata afatgjata me modele të njohura të sjelljes (RID, 2020). Ky nocion është vendosur në kuadër të kërcënimeve më të gjera hibride (Hoffman, 2007), për të cilat strategjia kombëtare kërkon një përgjigje më të integruar dhe më të koordinuar në nivel kombëtar, me role të qarta dhe mekanizma të qëndrueshmërisë.

Përkufizimi për NHMI-në sipas Shërbimit Evropian për Veprim të Jashtëm është(*The European External Action Service - EEAS*): "NHMI-ja përfaqëson një model të sjelljes kryesisht jo-ligjore që kërcënon ose ka potencial të ndikojë negativisht në vlerat, procedurat dhe proceset politike. Aktivitete të tilla janë të natyrës manipuluese, të kryera në mënyrë të qëllimshme dhe të koordinuar. Aktorët në këto aktivitete mund të jenë subjekte shtetërore ose joshtetërore, duke përfshirë ndërmjetësit, si brenda ashtu edhe jashtë territorit të tyre " (EEAS, 2025).

- *"Kryesisht jo-ligjore"* - kjo e bën të vështirë trajtimin e fenomenit përmes kuadrit ligjor ekzistues dhe krijon presion mbi ligjvënësit për të vendosur grupe të reja rregullash.

- *"Formular i sjelljes"* - ndërsa aktivitetet për të luftuar dezinformimin shpesh përqendrohen në përmbajtje dhe narrativa, ky përkufizim zhvendos fokusin nga përmbajtja në sjellje, pasi NHMI-ja përfaqëson manipulimin e qëllimshëm me informacione. Modeli i taktikave, teknikave dhe procedurave (*TTPs*) gjithashtu çon në identifikimin e aktorëve të kërcënimit.

- *"Kërcënon ose ndikon potencialisht mbi vlerat, procedurat dhe proceset politike"* - NHMI ka natyrë strategjike dhe përfshin çdo manipulim të informacionit që mund të shkaktojë dëm publik, ndërkaq prioritizohen katër fusha kryesore:

- Dezinformimi politik, i cili tenton të favorizojë njërën palë në konkurrencën politike ose të minojë besimin në institucione dhe procesin demokratik;
- Dezinformimi shëndetësor, i cili kërcënon komunitetet;
- Dezinformimi mjedisor, veçanërisht lidhur me ndryshimet klimatike;
- Dezinformimi që mund të përbëjë kërcënim për sigurinë ose të prishë rendin publik.

- *"Manipulues, i qëllimshëm dhe i koordinuar"* - Operacionet e NHMI-së përdorin taktika manipuluese për të mashtruar, çorientuar dhe destabilizuar qëllimin e vet. Qëllimet janë kryesisht shoqëritë demokratike, por ndërhyrjet dhe ndikimi i huaj janë të pranishme në nivel global, përfshirë vendet në zhvillim.

Aktorët e NHMI-së synojnë të shkaktojnë polarizim në shoqëri duke promovuar qëndrime ekstreme me qëllim thellimin e konflikteve, gjë që nga ana tjetër komplikon dialogun demokratik. Ata manipulojnë përmbajtjen duke modifikuar informacionin ose mediat autentike, të tilla si redaktimi i imazheve ose videove për hir të ndryshimit të kuptimit të tyre dhe krijojnë përmbajtje të fabrikuara, të tilla si faqet e internetit të rreme që imitojnë burime të ligjshme, video të rreme (deep fake) dhe materiale audio dhe vizuale të krijuara nga inteligjenca artificiale. Për më tepër, ato krijojnë narrativë të rremë, duke imituar personalitete dhe duke keqpërdorur profile diplomatike ose institucionale në rrjetet sociale; paralelisht, diskreditojnë burime konfidenciale dhe riformulojnë kontekstin për të hutuar audiencat, ndërsa amplifikimin e bëjnë përmes përdorimit të botëve, trollëve ose rrjeteve të koordinuara për të rritur artificialisht dukshmërinë dhe besueshmërinë e dezinformimit. Në të njëjtën kohë, përdoren mjete kibernetike, duke përfshirë hakimin dhe aktivitete të tjera për vjedhje, për modifikim ose fabrikim të informacioneve (Popovska V., 2024).

NHMI shfaqet përmes një bashkimi të narrativëve (si kornizohet tema dhe cilat emocione nxiten), kanaleve (mediat tradicionale, platformat online, aplikacionet e mesazheve) dhe teknikave (taktikat dhe veprimet e planifikuara). Shembuj tipikë janë:

- Sjellje e koordinuar jo autentike në rrjetet sociale (postime të harmonizuara, profile të rreme/"bote", krijimi i trendit artificial);
- "Hakimi dhe publikimi" i materialeve menjëherë para ngjarjeve të ndjeshme (zgjedhje, kriza), për të drejtuar vëmendjen dhe për të shkelur besimin;
- Organizatat ndërmjetëse dhe mediat me financim jo transparent, duke përfshirë praktikat e kapjes së mediave (kontrolli mbi politikat editoriale dhe pronësinë);
- Manipulimi i dukshmërisë së përmbajtjes në platforma (rangim i manipuluar, mbështetje qytetare "e organizuar", rritje artificiale e shtrirjes);
- Kombinimi me instrumente të tjera hibride (sulme kibernetike, presion ekonomik, përfshirje diplomatike) për efekt më të madh.

Këto praktika janë të vështira për t'u adresuar vetëm me masa që synojnë përmbajtjen individuale. Prandaj, **theksi vihet në vlerësimin e rrezikut dhe procedurat e qarta të reagimit midis autoriteteve shtetërore dhe platformave, në kuadër të politikës më të gjerë mbi kërcënimet hibride dhe rezistencën institucionale** (Blair-Simon K., 2025).

Prandaj, në përgjithësi **, shtetet në mënyrë të pavarur, në përputhje me vlerësimet e rrezikut, strategjitë e sigurisë kombëtare dhe doktrinat e mbrojtjes duhet të përcaktojnë, zbulojnë dhe kundërshtojnë këto lloje të kërcënimeve.**

Në kuadër të NATO-s, qasja përqendrohet në "kërcënimet e informacionit" – aktivitete të qëllimshme, të dëmshme, manipuluese dhe të koordinuara të kryera nga aktorë shtetërorë dhe jo-shtetërorë, duke përfshirë operacionet armiqësore informative, manipulimin e informacionit, ndërhyrjen nga aktorë të huaj dhe dezinformimin e shpërndarë përmes mediave tradicionale dhe sociale (NATO, 2020). Aleanca punon ngushtë me aleatët dhe partnerët për të kuptuar, parandaluar dhe ndërtuar qëndrueshmëri ndaj këtyre kërcënimeve informative. Përgjigjet e NATO-s përfshijnë masa proaktive afatshkurtra, afatmesme dhe afatgjata, bazuar në katër funksione kryesore: (1) të kuptuarit e mjedisit informativ (*Understand*), (2) parandalimi i efektivitetit të kërcënimeve informative (*Prevent*), (3) kufizimi dhe zbutja e incidenteve specifike informative dhe (*Contain and Mitigate*) dhe (4) rimëkëmbja dhe nxjerrja e mësimeve (*Recover*). **Komunikimi proaktiv është një nga mjetet kryesore për të luftuar kërcënimet e informacionit.** Aleanca e NATO-s komunikon me audiencën e synuar përmes kanaleve të ndryshme (faqja zyrtare e internetit, njoftimet editoriale dhe për shtyp, NATO Review, podkaste, profilet zyrtare të X, Facebook, Instagram, YouTube dhe LinkedIn), duke siguruar informacion të saktë që i ndihmon njerëzit të njohin dhe të kundërshtojnë kërcënimet e informacionit. Kjo qasje proaktive për shpjegimin dhe pastrimin paraprak të narrativave (*prebunking*) është në përputhje me kornizën info- ambientale dhe klasifikimin e llojeve të dezinformimit (Wardle & Derakhshan, 2017). Hulumtimet tregojnë se paralajmërimet e shkurtra para ekspozimit rrisin rezistencën ndaj narrativave manipuluese (Banas & Miller, 2013).

Rregulloret evropiane, të tilla si Akti për shërbime dixhitale (DSA) dhe Akti Evropian për Lirinë e Medias (EMFA), shtojnë një pikëpamje sistematike (European Commission, 2020): në vend të reagimeve të njëhershme ndaj përmbajtjes individuale, fokusi është në menaxhimin e rreziqeve sistemike, mbrojtjen e pluralizmit të medias dhe mekanizmat e raportimit dhe koordinimit ndërveprues (Blair-Simon K., 2025). Kjo nënkupton që përgjigja efektive ndaj NHMI-së duhet të kombinojë koordinimin institucional, protokollet operacionale dhe rezistencën e komunikimit, dhe jo vetëm ndalimet ligjore ose masat teknike.

1.2. Ndërhyrja në zgjedhje ndër operacionet më komplekse të NHMI-së

Një hulumtim i Eurobarometrit mbi qytetarinë dhe demokracinë nga dhjetori 2023 zbuloi se 81 përqind e qytetarëve të BE-së besojnë se ndërhyrja e huaj në sistemet demokratike është një problem serioz që duhet të adresohet, ndërsa 78 përqind janë të shqetësuar se dezinformimi mund të ndikojë në vendimet se si votojnë njerëzit (European Commission, 2023). Dikur i kufizuar në frikësim, mashtrim zgjedhor ose sulme të hakerëve, sot ndërhyrja përfshin gjithashtu shumë më tepër ndërveprime të pafajshme, por të përhapura dhe të përditshme. Një bisedë në dukje e padëmshme dhe e rastësishme tani mund të konsiderohet pjesë e një fushate për ndikim armiqësor.

Qeveria gjermane më 30 dhjetor 2024 akuzoi se Elon Musk po përpiqej të ndikonte në zgjedhje përmes mbështetjes së hapur për partinë politike Alternativa për Gjermaninë (*AfD*), pas së cilës administrata e Bundestagut në janar dhe shkurt 2025 filloi një kontroll nëse një mbështetje e tillë mund të konsiderohej një donacion i paligjshëm partiak. Musk më parë botoi një kolumnë në gazetën gjermane «*Welt am Sonntag*» duke lavdëruar *AfD* dhe më 9 janar 2025, ai mori pjesë në një bisedë të drejtpërdrejtë në IKS me bashkëkryetaren e partisë Alise Weidel (platforma ka mbi 200 milionë ndjekës). Paralelisht, Komisioni Evropian në kuadër të procedurës ekzistuese për shkeljen e Aktit Evropian të Shërbimeve Digjitale (*DSA*) kundër Iks (më 9 dhe 17 janar 2025) kreu kontrolle shtesë dhe kërkoi dokumentacion mbi algoritmet dhe bisedën live të zhvilluar (Reuters, 2025).

Pas shpërthimit të luftës në Ukrainë në vitin 2022, Rusia filloi një fushatë të gjerë dezinformimi që synonte destabilizimin e BE-së dhe anëtarëve të saj. Si përgjigje, BE vendosi sanksione kundër aseteve dhe aktorëve rusë të përfshirë në NHMI. Më 8 tetor 2024, u miratuan masa shtesë kufizuese kundër aktiviteteve destabilizuese të Rusisë, duke përfshirë minimin e proceseve zgjedhore, prishjen e funksionimit të institucioneve demokratike dhe sulmet e koordinuara me dezinformimin dhe ndërhyrjen e huaj.

Gjatë zgjedhjeve në Brazil në vitin 2022, dezinformatat e përhapura përmes *WhatsApp dhe Telegram* ndikuan ndjeshëm në qëndrimet e votuesve. Gjykata e Mbikëqyrjes Zgjedhore (*TSE*) shpesh kërkonte heqjen e përmbajtjes dhe u aktivizua një çatbot për kontrollin e fakteve. Hulumtimet kanë treguar se këto platforma kanë mundësuar shpërndarjen masive të informacionit të rremë, veçanërisht në lidhje me makinat elektronike të votimit, duke çuar në mosbesim në procesin zgjedhor dhe rritjen e tensioneve (Fondacioni Mozilla, 2024).

Shembuj të ndërhyrjes në proceset zgjedhore dhe proceset e tjera kryesore shtetërore vërehen gjithashtu në rajon.

Në zgjedhjet presidenciale të Rumanisë, të mbajtura më 24 nëntor 2024, kandidati ultra-nacionalist pro-rus Calin Gheorgescu udhëhoqi në raundin e parë me 22.94 për qind të votave. Ky rezultat hodhi poshtë sondazhet parazgjedhore, të cilat parashikonin që mbështetja e tij të ishte midis 5 dhe 10 për qind. Georgescu, një kritik i zëshëm i NATO-s dhe BE-së, tejkaloi kryeministrin në detyrë Marcel Ciolacu, i cili siguroi vetëm 19.5 përqind të votave, hera e parë në Rumaninë post-komuniste që një Social Demokrat (*PSD*) nuk arriti të kalonte në raundin e dytë. Fushata e Georgescu u shënua nga një rritje e dyshimtë e aktivitetit në mediat sociale, veçanërisht në Tic-Toc dhe Telegram, të nxitura nga ndikuesit e paguar dhe një rrjet i koordinuar i llogarive në platformat sociale. Shërbimet rumune të inteligjencës zbuluan se aktorët e lidhur me Rusinë luajtën një rol kryesor në amplifikimin e narrativave pro-ruse dhe anti-perëndimore. Tik-toku hoqi miliona llogari të rreme që promovonin mesazhet e Gheorgescu, edhe pse fushata tashmë kishte shkaktuar dëme të konsiderueshme. Vlerësimet e inteligjencës konfirmuan se shumë nga këto llogari ishin të lidhura me subjekte të lidhura me Rusinë, duke dëshmuar përfshirjen e drejtpërdrejtë të Moskës në manipulimin e opinionit publik. Më 6 dhjetor 2024, Gjykata Kushtetuese e Rumanisë ndërmori hapin e paprecedentë të anulimit të rezultateve të zgjedhjeve për shkak të parregullsive të përhapura dhe dyshimeve të besueshme për ndërhyrje të huaja

(House of Commons Library, 2024).

Gjatë një konference për shtyp në mars të vitit 2025, kryeministri i Kosovës Albin Kurti deklaroi se presidenti serb Aleksandar Vuçiq ndërhyri në zgjedhjet parlamentare në Kosovë përmes qeverisë serbe, shërbimeve të inteligjencës dhe grupeve të krimit të organizuar. Kurti gjithashtu përmendi se Milan Radojiçiq, ish-nënkryetar i partisë Lista Serbe, luajti një rol të rëndësishëm në ndërhyrje. Radojiçiq mori përgjegjësinë për organizimin e sulmit në fshatin Banjska në komunën e Zveçanit, me popullsi shumicë serbe, në veri të Kosovës, më 24 shtator 2023. Kosova ka kërkuar ekstradimin e tij nga Serbia. Në një reagim në Facebook, Lista Serbe hodhi poshtë akuzat nga Kurti dhe Rashiq, duke i quajtur ato «gënjeshtra brutale». «Lista Serbe është krenare që mori mbështetjen më të madhe nga populli serb dhe që, pavarësisht të gjitha presioneve, shantazheve dhe kërcënimeve, arriti të rezistojë falë unitetit të popullit tonë, duke dëshmuar edhe një herë se nuk do të ketë dorëzim», deklaruan nga partia. Misioni për Vëzhgimin e Zgjedhjeve të Bashkimit Evropian më 11 shkurt 2025, gjatë prezantimit të gjetjeve paraprake mbi zgjedhjet e mbajtura, deklaroi se Serbia kishte ndërhyrë në zgjedhje përmes presionit ndaj votuesve serbë në Kosovë (EU EOM, 2025).

Zgjedhjet lokale në Nikshiq në vitin 2021 shënuan një pikë kthese për Malin e Zi, veçanërisht për shkak të përfshirjes së fortë të Serbisë fqinje në fushatën zgjedhore. Prania e figurave të afërta ose anëtare të partisë qeverisëse të Serbisë, Partia Progresive Serbe (SNS), ka ngritur shqetësime. Disa prej tyre u ndaluan dhe të tjerëve iu ndalua hyrja në vend për shkak të dyshimit se kishin sjellë para për të blerë vota. Pas përfundimit të zgjedhjeve, Qyteti i Beogradit, siç premtoi në fushatë, i dhuroi dy milionë euro komunës së Nikshiqit, gjë që përforcoi më tej dyshimet për shkelje të integritetit zgjedhor dhe ndikimit të huaj (CDT, 2024).

Mali i Zi u përball me trazira politike pak para aderimit në NATO, por edhe më pas, të cilat ishin pasojë e çështjeve të ndryshme në dukje sociale ndërsa më të theksuara ishin ato që lidheshin me çështjet fetare. Faza e demoralizimit përfshiu një prani të madhe të informacionit të rremë, gjuhës së urrejtjes, dezinformimit dhe thirrjeve për mbrojtje kundër një armiku imagjinar. Në fushatën e dezinformimit, një portal në internet luajti një rol kryesor duke krijuar një kuant serioz të dezinformatave. Ueb portali, edhe pse nuk ka qenë i regjistruar në regjistrin e mediave, është paraqitur si media informative. Kështu, kanë krijuar shumë përmbajtje që synonin të provokonin një reagim emocional nga audienca, duke përdorur keqpërdorimin e konteksteve historike dhe lidhjen e Presidentit të Malit të Zi me regjimet fashiste të Luftës së Dytë Botërore. Media pro-Kremlinit "Sputnik" veproi në mënyrë të ngjashme. Rastet e dezinformimit nga këto dy portale u dokumentuan nga qendra e forenzikës digjitale në Podgoricë (IREX, 2023).

Nga ky këndvështrim, ndërhyrja nuk ka të bëjë aq shumë me mënyrën se si votohet, por me formësimin e motivimeve, qëllimeve dhe konteksteve në të cilat votuesit mendojnë për politikën. Dhe janë pikërisht këto procese – debatet, bindjet dhe mosmarrëveshjet kaotike - që janë një pjesë thelbësore e demokracisë.

1.3. Qasja e përgjegjshme dhe analitike e BE-së ndaj NHMI-së

Bashkimi Evropian ka zhvilluar një infrastrukturë gjithëpërfshirëse që mundëson operacionalizimin e aktiviteteve që synojnë ndërtimin e rezistencës ndaj ndikimit të huaj keqdashës. Kjo infrastrukturë bazohet në disa dokumente, rregullore dhe mekanizma strategjikë. Përmes këtyre instrumenteve, BE-ja jo vetëm që përcakton standardet për identifikimin dhe luftimin e ndërhyrjes së huaj dhe manipulimit të informacionit dhe kërcënimeve hibride, por gjithashtu krijon mekanizma operacionalë konkretë për koordinimin midis institucioneve, monitorimin e rreziqeve dhe angazhimin e sektorit privat dhe shoqërisë civile. Për më tepër, përmes Shërbimit Evropian për Veprim të Jashtëm (EEAS) dhe ekipeve të specializuara si EU Hybrid Fusion Cell dhe StratCom Task Forces, është e mundur të mblidhen, analizohen dhe shpërndahen informacione mbi ndikimet e mundshme në kohën e duhur, në mënyrë që të mbështeten shtetet anëtare dhe partnerët në zhvillimin e kapaciteteve të tyre të rezistencës. Ndërveprimi në rrjetet ndërkombëtare rrit rezistencën në një mjedis të ndërvarur (Keohane & Nye, 1998).

Ndër mekanizmat në dispozicion të Këshillit të BE-së janë:

- **Një grup mjetesh për përgjigje ndaj NHMI-së FIMI Toolbox, EEAS);**
- **Grup mjetesh hibride, duke përfshirë ekipet për reagim të shpejtë ndaj kërcënimeve hibride (Hybrid Toolbox; Hybrid Rapid Response Teams - HRRTs);**
- **Grupi i mjeteve të BE-së mbi Diplomacinë Kibernetike (EU Cyber Diplomacy Toolbox);**
- **Rrjeti Evropian për bashkëpunim në zgjedhje (European Cooperation Network on Elections - ECNE);**
- **Kodi për praktika kundër dezinformatave (Strengthened Code of Practice on Disinformation, 2022);**
- **Sistemi për alarmim të shpejtë (Rapid Alert System RAS);**
- **Opservatori Evropian për media digjitale (European Digital Media Observatory - EDMO).**

Për më tepër, BE-ja ka miratuar disa **akte dhe direktiva** me qëllim rritjen e përgjegjësisë së platformave online, forcimin e sigurisë kibernetike, qëndrueshmërinë e infrastrukturës digjitale dhe rregullimin e përdorimit të teknologjive të reja në komunikim. Këto legjislacione përfshijnë:

- **Akti për shërbime digjitale (Digital Services Act - Regulation (EU) 2022/2065);**
- **Akti për inteligjencën artificiale (Artificial Intelligence Act - Regulation (EU) 2024/1689);**

- **Direktiva për rezistencë për subjekte kritike (Directive (EU) 2022/2557);**
- **Direktiva për sigurinë e rrjetit dhe informacionit (NIS2 – Directive (EU) 2022/2555);**
- **Rregullorja për Transparencën dhe Synimin e Reklamimit Politik (Regulation (EU) 2024/900);**
- **Akti për lirinë e mediave në Evropë (European Media Freedom Act – Regulation (EU) 2024/1083).**

Këto masa janë përshkruar në konkluzionet e Këshillit të Evropës të majit 2024 për mbrojtjen e proceseve zgjedhore nga ndërhyrjet e huaja dhe në konkluzionet e Presidencës të majit 2025 për forcimin e rezistencës demokratike.

BE-ja ka zhvilluar dy mekanizma kryesorë për t'u marrë me ndikimin e informacionit të huaj: një set mjetesh për t'iu përgjigjur (*FIMI Toolbox*)dhe Sistemi për Alarmim të Shpejtë (*Rapid Alert System - RAS*), të cilat mund të ndërmerren dhe zbatohen duke iu përshtatur nevojave dhe kontekstit kombëtar (EU StratCom Task Force, 2022).

Grupi i mjeteve për përgjigje ndaj NHMI-së të krijuar nga Shërbimi Evropian për Veprim të Jashtëm është një mekanizëm kornizë konceptuale dhe operacionale, më shumë parandaluese sesa reaktive dhe bazohet në katër shtylla:

1. Ndërgjegjësimi i situatës - përmes teknikave të monitorimit, analizës dhe mbledhjes së informacionit nga burime publike ose burime të tjera të hapura (OSINT), identifikohen narrativat, burimet dhe metodat e manipulimit;
2. Qëndrueshmëria - ndërton kapacitetin e qytetarëve, mediave dhe institucioneve për të njohur dhe refuzuar dezinformimin;
3. Rregullativa - hartohen politika dhe mekanizma ligjorë për sanksionimin dhe parandalimin;
4. Aksioni i jashtëm - përgjigje diplomatike, mbështetja e partnerëve dhe koordinimi global.

Sistemi për Alarmim të Shpejtë (*RAS***)** është një platformë digjitale që funksionon si një alarm informacioni - kur zbulohet një fushatë dezinformimi, sistemi mundëson shkëmbimin e shpejtë të informacionit midis Shteteve Anëtare, institucioneve dhe partnerëve. Mekanizmi përfshin një rrjet të pikave qendrore kombëtare që janë të lidhura në kohë reale dhe mundëson integrimin e të dhënave nga media, verifikuesit e fakteve, burimet akademike dhe platformat e teknologjisë. Përgjigjet e koordinuara mund të jenë komunikimet publike, përgjigjet diplomatike ose ndërhyrjet teknike**.**

Shërbimi Evropian për Veprim të Jashtëm ka krijuar gjithashtu një **kornizë të përparuar analitike për kërcënimet nga NHMI-ja**, e cila mund të shërbejë si një model për mënyrën se si duhet të strukturohet procesi i monitorimit, analizës dhe shkëmbimit të informacionit midis institucioneve (EEAS, 2023; EEAS, 2024). Korniza analitike është një sistem i integruar që bashkon elementet metodologjike (ABCDE), elementet e procesit (cikli analitik), teknike (DISARM) dhe strukturore (STIX):

- **ABCDE.** Modeli kornizë ABCDE përfaqëson një qasje themelore për diferencimin e incidenteve nga NHMI-ja sipas pesë dimensioneve: Aktori (Actor), Sjellja (Behaviour), Shkalla (Degree) dhe Efekti (Effect). Zbatimi i tij në një kontekst kombëtar do të mundësonte krijimin e standardeve për analizën e incidenteve të NHMI-së, njohjen e modeleve të përsëritura dhe zhvillimin e kundërmasave.

Tabela 1: Kuadri ABCDE për analizën e NHMI-së

Element	Pyetje	Qëllimi
Aktor (Actor)	Cilët aktorë janë të përfshirë?	Të përcaktohet nëse incidenti ka të bëjë me një shtet të huaj apo aktor joshtetëror.
Sjellja (Behaviour)	Çfarë aktivitetesh janë vërejtur?	Të identifikohen provat për koordinim, qëllim dhe teknikat e përdorura.
Përmbajtja (Content)	Çfarë lloj përmbajtje po krijohet dhe shpërndahet?	Të përcaktohet nëse informacioni është mashtrues, manipulues apo pjesërisht i saktë.
Shkalla (Degree)	Si shpërndahet përmbajtja?	Analizoni audiencën e synuar dhe vëllimin e shpërndarjes.
Efekti (Effect)	Çfarë ndikimi ka dhe kë prek?	Vlerësoni dëmin aktual dhe seriozitetin e rastit.

- **Cikli analitik**. Shërbimi Evropian për Veprim të Jashtëm mbështetet në këtë kornizë duke krijuar një cikël analitik, i cili mundëson një proces strategjik dhe të vetë-qëndrueshëm të monitorimit, analizimit dhe përmirësimit të njohurive institucionale. Fazat e ciklit analitik përfshijnë:

1. Monitorimi Strategjik (Strategic Monitoring) - hartëzohet ekosistemi i burimeve të njohura të përdorura nga aktorët e kërcënimeve, monitorohen modelet e përforcimit dhe kanaleve të reja të shpërndarjes;
2. Prioritizimi dhe triazhi (Prioritisation and Triage) -zgjidhen incidentet me prioritet më të lartë, veçanërisht ato që kanë një rëndësi të drejtpërdrejtë politike ose të sigurisë;
3. Analiza e incidenteve dhe mbledhja e provave (Incident Analysis and Evidence Collection) - bëhet analiza e lidhjes së kanaleve dhe përmbajtjes, ndërsa provat arkivohen në përputhje me Rregulloren e Përgjithshme për Mbrojtjen e të Dhënave (General Data Protection Regulation - GDPR) dhe Protokollin e Berkeley për Hetimet Digjitale të bazuara në Burime të Hapura (Berkeley Protocol on Digital Open-Source Investigations);

4. Ndarja e njohurive (Knowledge Pooling and Sharing) - rezultatet ndahen me institucionet dhe partnerët përkatës në mënyrë që të reagojnë shpejt dhe të ndërtojnë vetëdijen kolektive;
5. Ndërgjegjësimi i situatës (Situational Awareness) -përditësohet një bazë të dhënash, shtohen aktorë dhe teknika të reja dhe përmes analizës krahasuese nxirren tendenca afatgjata.

- **DISARM**. Për të funksionalizuar elementin "B" të kornizës ABCDE, përkatësisht sjelljen e aktorëve që janë pjesë e NHMI-së, Shërbimi Evropian për Veprim të Jashtëm përdor kornizën DISARM**.** Është një sistem i zakonshëm, i hapur dhe i adaptueshëm për kategorizimin e teknikave, taktikave dhe procedurave (*TTPs*) të cilat i përdorin aktorët e kërcënimeve, duke lejuar identifikimin e teknikave dhe taktikave të tyre të përsëritura dhe zbulimin dhe përfundimin e hershëm të operacioneve të tyre. Kuadri DISARM ndan fazat e një incidenti të vetëm NHMI në:

6. Planifikim (Planning) - përcaktimi i qëllimit dhe ndikimit të pritshëm;
7. Përgatitja (Preparation) - krijimi i infrastrukturës dhe përzgjedhja e kanaleve;
8. Ekzekutimi (Execution) - zbatimi i operacionit përmes aktiviteteve të koordinuara;
9. Vlerësimi (Assessing) -matja e efektit dhe përshtatja e strategjisë.

- **STIX™**. Së fundi, për të siguruar shkëmbimin e informacionit mbi kërcënimet, Shërbimi Evropian i Veprimit të Jashtëm kodon incidentet NHMI në formatin STIX™ (*Structured Threat Information Expression*). Zbatimi i këtij formati lejon ndërveprimin midis institucioneve dhe integrimin e informacionit të pjesshëm në një tablo më të madhe analitike. Kështu, çdo narrativë ose teknikë e identifikuar kontribuon në krijimin e ndërgjegjësimit të situatës dhe paralajmërimit të hershëm. Ky format, i zhvilluar fillimisht për sigurinë kibernetike, lejon përfaqësimin e të gjitha objekteve dhe lidhjeve përkatëse në një incident të vetëm NHMI-së.

Tabela 2: Formati STIX™ (Structured Threat Information Expression)

Objekti STIX	Përshkrim
Incident (Incident)	Përmban informacion bazë në lidhje me incidentin (emri, përshkrimi, data e fillimit, qëllimi, etj.)
E vëzhguar (Observable)	URL ose skedar që është vërejtur në kuadër të incidentit.
Kanale - përhapja (Channels extension)	Çdo kanal komunikimi online ose offline (faqja e internetit, faqja e profilit ose e mediave sociale, stacioni televiziv, etj.) që publikon elementet e vëzhguara.
Identiteti (Identity)	Individë, organizata ose vendndodhje, përfshirë shtetet. Ai zakonisht mbulon objektivat e incidenteve.

Aktor kërcënimi (Threat Actor)	Përmban informacione në lidhje me aktorët që përbëjnë kërcënim.
Ngjarje - përhapja (Event (extension))	Përshkrimi i një ngjarjeje të vërtetë, si zgjedhje, emision, përvjetor, etj., për të siguruar kontekstin në të cilin mund të ndodhin incidente.
Cenueshmëria (Vulnerability)	Përshkrim i cenueshmërisë që do të përdorej për të mundësuar kryerjen e incidentit.
Gjuha - përhapja (Language (extension))	Gjuha/gjuhët e përdorura në incident.
Modeli i sulmit (Attack Pattern)	Përshkrimi i teknikave manipuluese (TTPs) të përdorura për të kryer sulmin.
Kursi i veprimit (Course of Action)	Përshkrimi i kundërmasave ndaj incidentit.
Narracion – përhapja (Narrative (extension))	Përshkrim i narrativave të përdorura në incidente. Narrativat mund të integrohen dhe të paraqiten si meta- dhe nën-narrativa.

Kuadri analitik i Shërbimit Evropian për Veprim të Jashtëm, i përshtatur për specifikat kombëtare dhe strukturën institucionale, mund të bëhet themeli i sistemit kombëtar për paralajmërim të hershëm dhe reagimit ndaj NHMI-së, i cili do t'u lejonte institucioneve të krijojnë një metodologji dhe terminologji të përbashkët për analizën e incidenteve të informacionit, të krijojnë një bazë të dhënash të unifikuar të aktorëve, teknikave dhe përmbajtjes, të mundësojnë përgjigje të koordinuara dhe në kohë, si dhe të zhvillojnë kapacitete parashikuese dhe parandaluese afatgjata.



KAPITULLI 2:

SITUATA DHE SFIDAT E REAGIMIT INSTITUCIONAL NDAJ NHMI-SË NË MAQEDONINË E VERIUT

2.1. Gjetjet e sintetizuara nga hulumtimi cilësor

2.1.1. Konsiderata dhe perceptime të përgjithshme

Ekziston vetëdije midis aktorëve shtetërorë në Maqedoninë e Veriut për çështjen e përgjithshme të kërcënimeve hibride, dezinformimit dhe potencialit për ndikim të dëmshëm të huaj. Është perceptuar se Maqedonia e Veriut është e vendosur në një mjedis rajonal shumë të ekspozuar, ku ndikimet e informacionit, veçanërisht ato me origjinë të huaj, shpesh bazohen në ndarjet ekzistuese politike dhe sociale. Megjithatë, **niveli i të kuptuarit të çështjes është i ndryshëm dhe, siç pritet, është më i lartë midis përfaqësuesve të komunitetit të sigurisë dhe inteligjencës**. Ndërhyrja e huaj dhe manipulimi me informacionin njihet si një fenomen kompleks dhe dinamik që ndodhet në kryqëzimin e politikave të sigurisë, informacionit dhe komunikimit. Por duke qenë se ky kërcënim nuk është përcaktuar në rregulloren e brendshme, asaj ende i mungon një mirëkuptim i unifikuar institucional. Disa palë të interesuara shtetërore identifikojnë NHMI-në kryesisht përmes një prizmi të sulmeve kibernetike, propagandës në internet dhe përmbajtjes manipuluese, ndërsa të tjerët e lidhin atë me forma më të gjera të ndikimit të huaj dhe praktikave destabilizuese të komunikimit. Prandaj, **ekziston një nevojë e caktuar për ndërhyrje në kornizën e ndërtimit të politikave**.

Në vend, **ekziston infrastrukturë themelore institucionale, por është e nevojshme të lidhen pikat e izoluara në një sistem që funksionon në** mënyrë koherente dhe me vendosmëri, me kompetenca dhe aktivitete të përcaktuara saktësisht. Megjithëse NHMI-ja perceptohet si një kërcënim real dhe në rritje për proceset demokratike dhe sigurinë kombëtare, institucionet në pjesën më të madhe i qasen asaj në mënyrë selektive dhe në varësi të kontekstit, me aktivitete të përqendruara kryesisht në situatat aktuale të krizës (proceset zgjedhore, fushatat e dezinformimit ose ngjarjet rajonale), sesa brenda një mekanizmi të vazhdueshëm, sistematik për parandalimin dhe qëndrueshmërinë. Jo të gjitha palët e interesuara e njohin rolin e tyre në sistemin më të gjerë, dhe shumica theksojnë mungesën e komunikimit dhe kujtesës institucionale, si dhe mungesën e kapaciteteve njerëzore dhe teknike. Shumica dërrmuese nuk i njohin institucionet e tyre as si mbajtëse të përgjegjësisë dhe as kompetenca në atë pjesë, që nënkupton se **nevojitet ndërhyrje edhe në nivelin strategjik dhe politik**.

Proceset e iniciuara në Ministrinë për Transformim Digjital në drejtim të përafrimit të Direktivave Evropiane për Sigurinë e Rrjetit dhe Aktit për Shërbimet Digjitale (*DSA*) **pritet të japin rezultate të forta në drejtim të rritjes së rezistencës kibernetike, ndërsabashkëpunimi tashmë i vendosur me vendet dhe organizatat partnere konsiderohet vendimtar në tejkalimin e sfidave**.

Shumica e **aktorëve shtetërorë nuk ishin të vetëdijshëm për ekzistencën e planit të veprimit në lidhje me Strategjinë për Ndërtimin e Rezistencës ndaj Kërcënimeve Hibride**, ndërsa disa theksuan se përgjegjësitë që u janë besuar atyre me strategjinë nuk janë pjesë e kompetencës së tyre institucionale. Megjithëse nuk dihet nëse ka një

mekanizëm për të monitoruar zbatimin e planit të veprimit në lidhje me Strategjinë, është e qartë se nuk ka arritur rezultatet e parashikuara, gjë që **kërkon analizë të thellë gjatë përgatitjes së dokumentit tjetër strategjik dhe/ose të veprimit në cikël**.

Kjo tregon se **institucionet shtetërore janë në faza të ndryshme të miratimit institucional të konceptit të NHMI-së:** nga ndërgjegjësimi bazë, përmes zhvillimit të kapaciteteve të brendshme, deri tek integrimi praktik në dokumentet strategjike dhe politikat operacionale. Kjo nënkupton që ndërgjegjësimi, njohuria dhe reagimi ndaj ndërhyrjes së huaj dhe manipulimit me informacionin është **një fushë në të cilën nevojitet përmirësimi**. Institucionet pranojnë se ndërtimi i qëndrueshmërisë sociale ndaj NHMI-së kërkon një qasje afatgjatë që shkon përtej kornizave administrative dhe teknike dhe mbështetet në partneritetin me sektorët akademikë dhe qytetarë dhe mediat. Prandaj, edukimi sistematik në fushën e **edukimit mediatik dhe digjital dhe komunikimi transparent dhe i përgjegjshëm** është thelbësor për ngritjen e nivelit të rezistencës ndaj këtij lloji të kërcënimit.

2.1.2. Organizimi dhe koordinimi institucional

Në kontekstin aktual institucional, ekziston nevoja për krijimin e një mekanizmi koordinimi sistematik dhe të qëndrueshëm midis aktorëve përkatës. Edhe pse ekzistojnë forma të caktuara të komunikimit ndërinstitucional, ato bazohen kryesisht në marrëdhëniet joformale dhe kontaktet personale, gjë që krijon rrezik për mospërputhje, transparencë të kufizuar dhe varësi nga kapacitetet individuale. Kjo qasje, edhe pse ndonjëherë efektive në një periudhë afatshkurtër, nuk siguron stabilitet dhe parashikueshmëri institucionale afatgjatë në proceset e vendimmarrjes dhe zbatimit. Megjithëse Strategjia për Ndërtimin e Rezistencës ndaj Kërcënimeve Hibride dhe Plani i saj i Veprimit parashikojnë krijimin e strukturave dhe mekanizmave për shkëmbimin e rregullt të informacionit dhe koordinimit, Këshilli Koordinues i Komunitetit të Inteligjencës së Sigurisë, i cili parashikohet zyrtarisht si një organ koordinues, nuk mban takime të rregullta dhe nuk ka rezultate të dukshme në fushën e NHMI-së.

Në mungesë të një mekanizmi aktiv të centralizuar, institucionet reagojnë ad hoc, brenda kompetencave të tyre, duke rezultuar në një sistem të fragmentuar reagimi. Institucionet individuale kryejnë aktivitete të kufizuara siç janë fushatat për edukim mediatik, monitorimi i përmbajtjes dezinformuese ose aktivitete që lidhen me mbrojtjen e infrastrukturës kritike të informacionit, por këto përpjekje zhvillohen në mënyrë të izoluar, pa një kornizë të përbashkët për koordinim dhe shkëmbim informacioni.

Kjo situatë nuk është rezultat i mungesës së vullnetit, por i roleve të përcaktuara qartë, kanaleve të komunikimit dhe procedurave të koordinimit. Si rezultat, reagimet ndaj dezinformimit dhe narrativeve me potencial për të ndikuar në publik varen nga iniciativa e departamenteve individuale ose personave/individëve, në vend të një mekanizmi sistematik për vlerësim dhe reagim.

Megjithatë, **ekziston potenciali për krijimin e një rrjeti funksional të pikave të kontaktit institucional, i cili do të mundësonte komunikim dhe shkëmbim më të**

shpejtë të informacionit në rast të një incidenti ose krize informacioni. Një model i tillë mund të përfaqësojë një hap kalimtar drejt vendosjes së koordinimit të centralizuar, të vendosur në strukturat ekzistuese shtetërore ose duke krijuar një institucion të ri, me protokolle dhe përgjegjësi të përcaktuara qartë.

2.1.3. Kuadri legjislativ dhe strategjik

Megjithëse janë bërë hapa të rëndësishëm në vitet e fundit drejt përcaktimit të politikave dhe strategjive kombëtare në lidhje me rezistencën ndaj kërcënimeve hibride dhe të informacionit, kuadri ligjor dhe institucional për trajtimin e NHMI-së, ende nuk është krijuar plotësisht. Ka dokumente përkatëse, kryesisht Strategjia Kombëtare për Ndërtimin e Rezistencës dhe Ballafaqimin me Kërcënimet Hibride (2021–2025), Strategjia Kombëtare e Sigurisë Kibernetike 2025-2028, Strategjia e Reformës së Administratës Publike 2023-2030, si dhe aktivitetet e disa ministrive të linjës dhe organeve rregullatore, por funksionalizimi i tyre është i kufizuar dhe reciprokisht jokonsistent.

Nuk ka ndarje të qartë të përgjegjësive në fushën e parandalimit, monitorimit dhe reagimit ndaj shfaqjes së NHMI-së, si dhe nuk ka një mekanizëm për raportim dhe shkëmbim të koordinuar të informacionit midis institucioneve. Si rezultat, disa nga masat e parashikuara në Planin e Veprimit të Strategjisë për Ndërtimin e Rezistencës dhe Ballafaqimin me Kërcënimet Hibride nuk janë zbatuar ose zbatohen pjesërisht, kryesisht në nivel sektorial.

Sa i përket aspektit normativ, ligjet ekzistuese nuk i njohin format specifike të ndikimit të informacionit të huaj, por përqendrohen në fusha të ngjashme: rregullimi i mediave, siguria kibernetike, mbrojtja e të dhënave personale dhe proceset zgjedhore. Kjo krijon një mjedis rregullator të fragmentuar, në të cilin disa aspekte të NHMI-së mbeten jashtë një kompetence institucionale të përcaktuar qartë, pa një qasje të integruar.

Megjithatë, kuadri strategjik ekzistues është një bazë e mirë për zhvillimin e mëtejshëm. Është e nevojshme të bëhet lidhja e dokumenteve strategjike dhe përditësimi i tyre në funksion të sfidave të reja, si dhe krijimi i një dokumenti të vetëm kombëtar që do të integronte aspektet e edukimit mediatik, sigurisë digjitale, komunikimit strategjik dhe parandalimit të manipulimeve të huaja me ndikimin e informacionit dhe formave të komunikimit.

2.1.4. Kapacitetet dhe burimet

Institucionet përgjegjëse për aktivitetet e lidhura me NHMI-në përballen me burime të kufizuara njerëzore, teknike dhe financiare. Në shumicën e institucioneve, nuk ka departamente ose individë të veçantë me detyra të përcaktuara për monitorimin dhe analizimin e ndikimeve të informacionit, dhe kapacitetet ekzistuese shpërndahen më shpesh midis njësive të ndryshme organizative.

Mungon edukimi i vazhdueshëm për punonjësit e administratës publike në fushën e edukimit mediatik dhe edukimit digjital, aftësitë e analizës së informacionit dhe të kuptuarit e kërcënimeve hibride. Megjithëse disa programe trajnimi janë zbatuar në vitet e fundit (p.sh.

në kuadër të NATO-s, BE-së dhe partneriteteve bilaterale), ato nuk janë të sistematizuara dhe rrallë janë multisektoriale.

Burimet teknike, veçanërisht për monitorimin dhe analizimin e përmbajtjes në internet, janë të kufizuara dhe shkëmbimi i informacionit midis institucioneve shpesh mbështetet në kontakte joformale. Është e njohur që sektorët civilë dhe mediatikë kanë mjete dhe ekspertizë përkatëse që shteti mund t'i integrojë në mënyrë më efektive në përpjekjet e përbashkëta për të monitoruar dhe analizuar fushatat e dezinformimit.

Në këtë kontekst, **theksohet nevoja për zhvillimin e një sistemi kombëtar për paralajmërim të hershëm dhe për të krijuar një pikë të vetme referimi për koordinimin e aktiviteteve që lidhen me manipulimet e informacionit, e cila do të lidhte burimet ekzistuese institucionale dhe joqeveritare**.

2.1.5. Perceptimi i mundësive dhe sugjerime për përmirësim

Pavarësisht kufizimeve të perceptuara, më shumë mundësi dhe potenciale pozitive shihen për të rritur reagimin institucional ndaj NHMI-së:

- **Përcaktimi i qartë i roleve dhe kompetencave përmes rishikimit dhe përditësimit të dokumenteve strategjike ekzistuese dhe prezantimit të protokolleve operacionale për bashkëpunimin ndërinstitucional;**
- **Krijimi i një mekanizmi koordinimi të formalizuar ose forcimi i Këshillit ekzistues për Koordinim të Komunitetit të Inteligjencës së Sigurisë me detyra specifike për monitorim, analizë dhe raportim për NHMI-në;**
- **Krijimi i një sistemi për trajnim të vazhdueshëm dhe shkëmbim të rregulluar të përvojave ndërmjet institucioneve, mediave dhe komunitetit akademik;**
- **Integrimi dhe promovimi i edukimit mediatik dhe rezistencës digjitale si një komponent i përhershëm në programet arsimore dhe administrative;**
- **Thellimi i bashkëpunimit ndërkombëtar, në veçanti me NATO-n, BE-në, KiE-në, Qendrën hibride në Helsinki (Hybrid CoE) dhe nisma të tjera partnere për të luftuar dezinformimin;**
- **Mbështetje për partneritetin me organizatat akademike, qytetare dhe mediatike, si një burim për kontrollin e fakteve dhe zbulimin e tendencave të dezinformimit.**

2.1.6. Sfidat kryesore

Bazuar në të gjitha diskutimet, janë identifikuar disa sfida sistematike që kufizojnë aftësinë e shtetit për përballje me NHMI-në.

Tabela 3: Sfidat sistematike për përgjigjen ndaj NHMI-së

Fusha	Sfida kryesore
Diskriminimi institucional	Mungesa e një mekanizmi aktiv koordinimi dhe ndarja e qartë e roleve midis institucioneve.
Kapacitetet dhe burimet	Numri i pamjaftueshëm i stafit të trajnuar, mjetet e kufizuara teknike dhe shkëmbimi i dobët ndër-sektorial.
Kuadri ligjor	Mosekzistenca e një baze ligjore që adreson drejtpërdrejt NHMI-në; mbivendosja e kompetencave.
Shkëmbimi i informacionit	Komunikimi joformal dhe mungesa e standardeve për raportim dhe koordinim.
Qëndrueshmëria sociale	Edukimi i pamjaftueshëm mediatik dhe niveli i ulët i besimit në institucione.
Bashkëpunim ndërkombëtar	Përdorimi i kufizuar i iniciativave ekzistuese të NATO-s, BE-së dhe partnerëve për luftë kundër dezinformatave.

2.2. Analiza e statusit të sistemit (*GAP Analysis*)

Ky seksion sistematizon boshllëqet kritike midis kuadrit ekzistues strategjik dhe ligjor dhe praktikës aktuale institucionale për t'iu përgjigjur ndërhyrjes së huaj dhe manipulimit me informacionin. Fushat pasqyrohen drejtpërdrejt nga temat e hulumtimit cilësor (2.1.), për të siguruar një tranzicion të pastër nga "ku jemi" në "çfarë na mungon" dhe më vonë në "çfarë duhet të bëjmë" (Kapitujt 3 dhe 4). Analiza u përgatit duke krahasuar: (a) gjetjet nga grupet e fokusit dhe intervistat (rutinat, proceset, kapacitetet) dhe (b) politikat dhe strategjitë ekzistuese dhe struktura institucionale formale. Çdo fushë vlerësohet për tre çështje: çfarë mungon (boshllëku), cila është pasoja dhe cila është masa e nevojshme.

2.2.1. Organizimi dhe koordinimi institucional

Boshllëku	Pasoja	Masa
Pikat fokale pjesërisht të formalizuara - nëpunësit për komunikim, me funksionim të pabarabartë dhe linja të paqarta të raportimit; Mungesa e procedurave standarde të unifikuara të funksionimit (SOPs) dhe rutinat për koordinimin ndërinstitucional për NHMI; Ka kanale komunikimi, por ato nuk janë të institucionalizuara: nuk ka procedura të qarta, rutina dhe transportues përgjegjës, vetëdije të pamjaftueshme për përdorimin e tyre dhe zbatim praktik të pabarabartë për shkëmbimin e rregullt dhe të strukturuar të informacionit, pikëpamjeve dhe rekomandimeve midis palëve të interesuara; Nuk janë zhvilluar procedura të qarta (SOPs) për trajtimin e skenarëve të ndryshëm, rasteve të përshkallëzimit ose situatave të krizës; Informime të shkurtra dhe të parregulluara mbi situatën, për të ofruar një pamje të konsoliduar dhe të përditësuar të kushteve aktuale;	Vështirësi në ndarjen në kohë të informacionit, planifikimin e përbashkët, vendimmarrjen dhe veprimin e sinkronizuar, veçanërisht në situata që kërkojnë vlerësim të saktë të rrezikut dhe reagim të shpejtë; Improvizimi pa të dhëna përkatëse dhe të sakta dhe përgjigje të parakohshme dhe joefektive; Reagime ad-hoc ndaj një kërcënimi ose incidenti - institucione të ndryshme reagojnë veçmas, pa një strategji dhe komunikim të koordinuar, të cilat mund të çojnë në konfuzion midis publikut dhe ulje të besimit në institucione; Duplikimi i përpjekjeve pa kompetenca të ndara qartë - institucione të ndryshme mund të ndërmarrin aktivitete të ngjashme pa qenë të vetëdijshëm për atë që konsumon burime dhe e bën procesin e analizës dhe vendimmarrjes më të vështirë; Mesazhe të paharmonizuara për publikun që janë thelbësore për menaxhimin e perceptimit publik dhe ruajtjen e stabilitetit shoqëror.	Pikat fokale në çdo institucion përkatës, si kontakte parësore në rrjetin ndërinstitucional, me kompetenca të qarta për koordinim dhe komunikim për shkëmbimin e shpejtë të informacionit, fillimin e aktiviteteve të përbashkëta dhe informimin në kohë të vendimmarrësve; Përdorimi i njëtrajtshëm dhe rutinë i kanaleve dhe mjeteve për koordinim, me bartës të qartë, shkaktarë të kohës dhe procedura për informim dhe referim të rregullt dhe urgjent në institucionet përkatëse; Procedurat standarde operative për identifikimin e incidenteve, vlerësimin e tyre sipas kritereve të paracaktuara dhe reagimin e koordinuar institucional për lloje të ndryshme të situatave (hapat për komunikimin e brendshëm, aktivizimin e pikave të kontaktit, informimin e publikut dhe përshkallëzimin në nivele më të larta të vendimmarrjes); Informime të rregullta të situatës midis institucioneve për vlerësimet aktuale të rrezikut, analizat e incidenteve të mëparshme dhe rekomandimet për të përmirësuar koordinimin.

2.2.2. Kuadri strategjik (operacionalizimi)

Boshllëku	Pasoja	Masa
Strategjitë ekzistojnë, por korniza operacionale për NHMI-në është e pamjaftueshme: nuk ka një nocion të përbashkët pune, rolet dhe kompetencat janë të pasakta dhe procedurat rrallë reduktohen në protokolle dhe tregues.	Pasiguria "kush udhëheq" në një incident, kompetenca të mbivendosura dhe vendime të ngadalta; Rrezik nga mbirregullimi për shkak të proceseve të paqarta.	Kuadri operacional (përkufizimi i punës, harta e roleve dhe përgjegjësive, listat e kontrollit dhe skenarët, modelet e vendimeve dhe mesazhet publike), mbështetur nga aktet nënligjore dhe udhëzimet, në vend të menjëherë një ligji të ri.

2.2.3. Kapacitetet dhe burimet

Boshllëku	Pasoja	Masa
Staf i kufizuar në profilet kryesore (OSINT, analitikë të dhënash, komunikim strategjik); Mungesa e mjeteve të përbashkëta për monitorim dhe analizë; Politika e kujtesës institucionale në mungesë.	Varësia nga individë; Mbulimi i pabarabartë i rrezikut, detektimi i ngadaltë dhe cilësia e dobët e analizës; Mungesa e kujtesës institucionale.	Plan për trajnime sipas niveleve (bazë – i avancuar – i specializuar); Organizimi i trajnimeve të rregullta për komunikim në krizë për të siguruar qëndrueshmëri dhe besueshmëri në mesazhet publike; Institucionalizimi i një "grupi mjetesh" qendror me mbështetje teknike dhe licenca; Praktikat e formalizuara për transferimin dhe ruajtjen e njohurive (leksione, baza të njohurive, mentorim).

2.2.4. Standardet për shkëmbimin e informacioneve

Boshllëku	Pasoja	Masa
Shkëmbimi i informacionit është kryesisht informal; Asnjë shabllon standard për incidente (fusha minimale dhe metadata); Nuk ka depo qendrore.	Pasqyrë e pjesshme dhe humbja e të dhënave; Versione paralele të të njëjtave analiza; Reagimi i vonuar i përbashkët.	Modeli standard për raportimin dhe monitorimin e incidenteve; - Depo e përbashkët me kontrolle për qasje për shkëmbimin e informacionit; Kontakti kombëtar i emëruar për Sistemin për Alarmim të Shpejtë të BE-së (RAS) (aty ku është e aplikueshme).

2.2.5. Qëndrueshmëria e komunikimit dhe edukimi

Boshllëku	Pasoja	Masa
Mungon komunikimi sistematik parandalues (prebunking) dhe korrigjues (debunking), si dhe udhëzimet e përbashkëta për transparencë; Edukimi mediatik dhe digjital i ulët në sektorin publik.	Një boshllëk në debatin publik që mbushet lehtësisht me narrativa manipuluese; Rënie e besimit dhe cenueshmëri më e madhe.	Procedurat e shkurtra të funksionimit të standardeve të komunikimit (kush, kur, si mesazh); Mesazhe parandaluese për narrativat e pritshme (para zgjedhjeve ose krizave); Programe për edukim mediatik dhe digjital dhe partneritetet e formalizuara me akademinë, organizatat e shoqërisë civile dhe mediat.

2.2.6. Monitorimi dhe vlerësimi

Boshllëku	Pasoja	Masa
Mungon grupi i indikatorëve kryesorë të performancës dhe rutina për raportimin mujor ose tremujor; Masat rrallë monitorohen përmes rezultateve.	Është e vështirë të matet efekti; Mësim i kufizuar institucional dhe argumentim i dobët për burimet e nevojshme.	Paketë me tregues kryesorë të performancës sipas fushave (koordinimi, kapacitetet, reagimi, komunikimi); Përmbledhje tremujore, raport vjetor dhe revizion i masave.



KAPITULLI 3:

PËRVOJAT KRAHASUESE DHE MODELET E REAGIMIT NDAJ NHMI

Analiza krahasuese e qasjeve të ndryshme kombëtare bën të mundur identifikimin e praktikave të mira, dobësive dhe potencialeve të përshtatjes në kontekstin lokal. Shfaqja tabelare sistemon zgjidhjet institucionale që zbatojnë vende të ndryshme për ballafaqim me ndërhyrjen e huaj dhe manipulimin e informacionit. Duke krahasuar kornizat ligjore, mekanizmat operativë, rolin e shërbimeve të sigurisë, organeve të pavarura dhe shoqërisë civile, fitohet një pasqyrë më e qartë se cilat modele kanë rezultuar efektive dhe cilat përballen me kufizime strukturore ose politike.

Për më tepër, kjo analizë lejon shqyrtimin kritik të shkallës së integrimit midis institucioneve të ndryshme – nga shërbimet e inteligjencës deri te rregullatorët e mediave dhe aftësinë e tyre për të vepruar në mënyrë të koordinuar. Në një natyrë që ndryshon me shpejtësi të kërcënimeve, fleksibiliteti dhe qasja ndërdisiplinore janë thelbësore. Prandaj, prezantimi tabelar nuk shërben vetëm si një mjet analitik, por edhe si një burim praktik për krijimin e rekomandimeve për një kornizë institucionale të zbatueshme për Maqedoninë e Veriut.

Tabela 4: Shfaqja e sistematizuar e modeleve kombëtare për përgjigje ndaj NHMI-së

Vendi / Organizata	Institucioni / Modeli	Lloji i strukturës	Funksionet kryesore	Burimi
Franca	VIGINUM	Shërbim publik pranë Kryeministrit	OSINT, analiza e ndikimit digjital, koordinimi ndërministror	https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
Gjermania	FIMI-ISAC	Rrjeti i organizatave (joformale)	Shkëmbimi i informacionit, mbështetja e organeve zgjedhore, mediave dhe sektorit civil	https://neweasterneurope.eu/state-responses-to-fimi-and-recommendations-for-resilience/
Suedia	Agjencia për Mbrojtje Psikologjike	Agjenci e pavarur qeveritare	Monitorim, edukim, mbështetje për mediat dhe institucionet publike	https://cospr.org/evolving-threat-of-foreign-information-manipulation-and-interference-fimi-critical-insights-from-3rd-eeas-report/
Finlanda	Strategjia Kombëtare për edukim mediatik	Modeli arsimor dhe qeveritar-institucional	Arsimi, fushata publike, hulumtime	https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU%282021%29653632_EN.pdf
Estonia	Qendra për komunikim strategjik	Zyrë qeveritare	Parandalimi i dezinformatave, edukimi mediatik, rezistenca digjitale	https://www.hybridcoe.fi/

Lituania	Strategjia e plotë për mbrojtje, MPB, njësitë strategjike të komunikimit	Modeli i të gjithë qeverisjes dhe i gjithë shoqërisë	Qëndrueshmëria civile dhe informative, komunikime strategjike, mbrojtja kibernetike, qëndrueshmëria e informacionit, komunikimi strategjik, mbrojtja kibernetike	https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323902/lithuanias-total-defense-review/
Polonia	Këshill për rezistencë, INFO OPS Polska, FIMI-ISAC (Integritet zgjedhor)	Koordinimi me shumë faktorë (qeveria + shoqëria civile)	Mbrojtja e zgjedhjeve, ndërgjegjësimi i publikut, njoftime për incidentet, koordinimi strategjik	https://infoops.pl/foreign-information-manipulation-and-interference-threats-and-answers-in-poland/
Republika Çeke	Koordinimi qeveritar për çështjet strategjike, BIS, FIMI-ISAC	Koordinimi qeveritar plus një komunitet sigurie	Siguria kibernetike, dezinformimi, zgjedhjet, monitorimi, arsimi	https://www.informedsociety.cz/wp-content/uploads/2024/10/EN_Safeguarding_Democracy_2024-09-26.pdf
Sllovakia	Qendra për përballje me kërcënimet hibride (CCHT)	Njësi pranë Ministrisë së Punëve të Brendshme	Monitorimi, komunikime strategjike, edukim, përditësimi i rregulloreve	https://www.hybridnehrozby.sk/ccht/
Ukraina	Qendra për komunikim strategjik	Struktura qeveritare dhe ushtarake	Kundër-propaganda, analiza e ndikimit, bashkëpunimi ndërkombëtar	https://www.hybridcoe.fi/
Rumania	Iniciativat kombëtare për mbrojtjen e zgjedhjeve dhe monitorimin e zgjedhjeve me IA	Strategjia e Qeverisë + trupat rregullatore	Monitorimi i Tik-tok, manipulime me IA, siguria e zgjedhjeve	https://visegradinsight.eu/safeguarding-democracy-against-information-manipulation-and-hybrid-threats/
Mali i Zi	Ministria e Punëve të Jashtme (Memorandum Mirëkuptimi me Shtetet e Bashkuara të Amerikës), CDT, Strategjia e Medias 2023–2027	Koordinimi i qeverisë dhe shoqëria civile	Dezinformata, monitorim, reforma legjislative, transparencë, mbrojtja e proceseve zgjedhore	https://www.gov.me/en/article/memorandum-of-understanding-signed-between-the-ministry-of-foreign-affairs-of-montenegro-and-the-us-department-of-state-close-cooperation-for-more-effective-fight-against-disinformation
BE	EEAS / EUvsDisinfo	Institucion pan-evropian	Arkivi i dezinformatave, përgjigjeve diplomatike, sanksioneve	https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

NATO	Ekipet për mbështetje kundër sulmeve hibride	Platforma shumëkombëshe	Mbështetja e Shteteve Anëtare, analizë, komunikimi strategjik	https://www.nato.int/cps/en/natohq/topics_156338.htm
SHBA	Qendra Globale e Angazhimit (GEC)	Platforma ndërinstitucionale	Analiza, partneritete, komunikim strategjik	https://govfacts.org/federal/eop/how-the-national-security-council-fights-foreign-disinformation-campaigns/
Kanada	Mekanizëm për Reagim të Shpejtë (RRM)	Platforma qeveritare + Koordinimi i G7	Monitorim, edukim publik, koordinim ndërkombëtar	https://2021-2025.state.gov/the-framework-to-counter-foreign-state-information-manipulation/
Tajvan	Programet Kombëtare për Qëndrueshmëri Digjitale	Strategjia e Qeverisë + Sektori Civil	Zgjidhjet teknologjike, edukimi, mbrojtja e zgjedhjeve	https://neweasterneurope.eu/state-responses-to-fimi-and-recommendations-for-resilience/

Më poshtë janë dhënë pesë modele që, edhe pse të ndryshme në formë institucionale, ndajnë karakteristika të përbashkëta: kapaciteti qendror/kryesor, rrjeti i pikave fokale, protokollet (*SOPs*), vlerësimi i rregullt i rrezikut dhe komunikimi publik i ngulitur.

3.1. Estonia: një shtet digjital me rutina ndërgjegjësimi dhe koordinimi

Estonia e bazon rezistencën institucionale në një qasje "digjitale si standard" në administratën publike,në të cilën menaxhimi me (meta) të dhënave dhe qasja në to është një pjesë standarde e punës së përditshme. Përgjigja ndaj kërcënimeve të informacionit kryhet përmes Qendrës për Komunikim Strategjik në Qeveri dhe ritualizohet: informime të shkurtra, fikse të situatës (1–2 faqe) që përgatiten dhe shpërndahen rregullisht; pika fokale në ministri, agjenci dhe infrastrukturë kritike që kanë detyra të qarta raportimi dhe përshkallëzimi; dhe ushtrime simulimi në tryezë (*table-top - TTX*) që mbahen çdo vit, shpesh para periudhave të ndjeshme (zgjedhje, tensione gjeopolitike, etj.).

Proceset mbështeten në formate të standardizuara: shabllone për incidente me fusha minimale (data/koha, burimi, përshkrimi, probabiliteti/ndikimi, masat e marra), fjalori i përbashkët i termave dhe metadata minimale teknike.

Një tipar i rëndësishëm është bashkimi i funksioneve teknike dhe të komunikimit: ekipet e komunikimit TIK/kibernetik dhe publik ulen rregullisht në të njëjtën tryezë, gjë që zvogëlon hendekun midis gjetjeve teknike dhe treguesve dhe një mesazhi dhe njoftimi të harmonizuar të komunikimit.

Pikat e forta	Pikat e dobëta/Rreziqet
Disiplina në rutinat, ndërveprimi, shkëmbimi i shpejtë.	Mbështetja e lartë në sistemet dixhitale; nevoja për të ruajtur në mënyrë të vazhdueshme standardet dhe për të planifikuar investimet dhe kostot operative (CAPEX /OPEX) për mjetet dhe mirëmbajtjen.

3.2. Franca (Viginum): kapaciteti kryesor i qeverisë kundër ndërhyrjeve digjitale

Viginum (*Viginum*) është një shembull i kapacitetit të centralizuar operacional të ndërtuar në arkitekturën qeveritare. Ekipi është i vogël, i profesionalizuar dhe vepron nën një mandat të qartë: vëzhgimi i hapësirës digjitale për ndërhyrje të huaj, sinteza analitike dhe paralajmërimi i linjave kur plotësohet një kriter (periudha zgjedhore ose krize, ndikim i rëndësishëm).

Puna është e protokolluar në mënyrë rigoroze: nivelet e sinjalit (në mënyrë të → konsiderueshme kritike), afatet kohore të raportimit, matricat e transportuesve përgjegjës dhe formatet e materialeve të gatshme për përdorim (Pyetje dhe Përgjigje, lista me fakte, linja e mesazheve). Parimi është të sigurohet ndërveprimi me ministritë dhe rregullatorët e ndryshëm pa krijuar një hierarki paralele. Për sa i përket transparencës, modeli praktikon informimin publik "minimalisht të nevojshëm", të mjaftueshëm për të vënë në dukje rrezikun pa amplifikuar narrativën.

Pikat e forta	Pikat e dobëta/Rreziqet
Mandat i qartë, linjë e shpejtë "sinjal vendim mesazh".	Centralizimi kërkon besim të vazhdueshëm ndërministror; ekspozimi i tepërt i publikut mund të hapë polemika të panevojshme.

3.3. Polonia: vlerësimi ndër-sektorial i rrezikut dhe informimet tremujore

Modeli polak përcakton vlerësimet e rrezikut si një motor koordinimi. Shërbimet e sigurisë, departamentet e TIK-ut dhe ekipet e komunikimit rregullisht kryqëzojnë gjetjet e referencës

dhe i kthejnë ato në matrica rreziku (probabiliteti x ndikimi), me masa të shkurtra zbutëse dhe transportues. Këto matrica nuk janë një tepricë administrative, por një mjet pune për informime tremujore, ku miratohen korrigjime të vogla, por të vazhdueshme: azhurnimi i procedurave të funksionimit standard sipas skenarëve të ndryshëm, ushtrimet e planifikimit, përafrimi i mesazheve.

Një element i rëndësishëm është kanali për koordinimin ndërshtetëror: kur një rast ka implikime ndërkufitare, ekziston një zakon i angazhimit të Sistemit për Alarmim tëShpejtë (*RAS*), jo për të zhvendosur përgjegjësinë, por për të koordinuar dritaret e kohës së informacionit dhe reagimit.

Pikat e forta	Pikat e dobëta/Rreziqet
Ritmi dhe kultura e parashikueshme e vlerësimit të përbashkët; transportueshmëria e lehtë e formatit.	Rreziku i një qasjeje "thjesht të shënohet si e kryer" nëse informimet reduktohen në një formalitet të thjeshtë; nevojitet lidership që këmbëngul në rezultate të zbatueshme.

3.4. Suedi: Agjencia për Mbrojtje Psikologjike

Agjencia Suedeze e Mbrojtjes Psikologjike institucionalizon forcimin e rezistencës sociale përmes trajnimit, këshillimit dhe mbështetjes operacionale. Mjedisi është horizontal: Agjencia nuk është një qendër mohimi, por përkundrazi ndihmon në rritjen e kapacitetit, i cili ndihmon institucionet e linjës të komunikojnë me publikun në situata komplekse (nga operacionet me ndikim deri te ngjarjet e krizës).

Praktikat kryesore janë katalogët e trajnimit (nga modulet themelore në ato të specializuara për ekipet e komunikimit, analistët, menaxherët), udhëzimet për komunikimin publik në periudha zgjedhore dhe krize (formulimi i mesazheve pa amplifikim, puna me mediat, standardet vizuale) dhe rishikimet pas ngjarjes (*after-action review*) që ofrojnë kujtesë institucionale dhe mësim.

Pikat e forta	Pikat e dobëta/Rreziqet
Fokus i qëndrueshëm në kompetencat dhe të mësuarit afatgjatë; besimi i publikut për shkak të rolit këshillues (jo policor).	Suksesi varet nga vullnetarizmi dhe hapja e institucioneve të linjës. Nevojiten kritere të qarta për prioritetet.

3.5. Finlanda: edukimi, partneritete dhe komunikime parandaluese

Finlanda e trajton mjedisin e informacionit si një kapacitet publik dhe investon në programet e edukimit mediatik dhe informativ për administratën publike, mësimdhënësit, nxënësit, gazetarët dhe komunitetet lokale. Paralelisht, zhvillohen komunikime parandaluese (*prebunking*): cikle të shkurtra, të përsëritura të mesazheve që synojnë narrativat e pritshme para zgjedhjeve, referendumeve ose ngjarjeve të krizës.

Metodologjikisht, qasja finlandeze mbështetet në bashkë-dizajnimin me shërbimin publik, sektorin akademik dhe civil, gjë që rrit legjitimitetin dhe mbulimin. Mesazhet testohen në qartësi dhe besim, në vend se vetëm në arritje, dhe tregues të tillë si mirëkuptimi, besimi dhe "koha për korrigjim" maten rregullisht. Kjo krijon një kulturë në të cilën institucionet publike posedojnë kompetencë komunikimi dhe nuk mbështeten vetëm në korrigjimin emergjent në një krizë.

Pikat e forta	Pikat e dobëta/Rreziqet
Legjitimitet dhe partneritete të larta sociale; matshmëria e efekteve.	Cikli më i ngadaltë i rezultateve; nevojitet mbështetje afatgjatë dhe konsensus politik për programet.



KAPITULLI 4:
OPSIONET PËR POLITIKËN E REAGIMIT NDAJ NHMI-SË NË MAQEDONINË E VERIUT

Ky kapitull ofron tre arkitektura realiste për reagimin sistematik ndaj NHMI-së. Qëllimi është të vendoset një zgjedhje e qartë midis shtigjeve të ndryshme, secila me funksione, avantazhe dhe kufizime të njohura.

4.1. Opsioni A: Qendra e Pavarur Kombëtare për Qëndrueshmëri

Organizimi i menaxhimit

Subjekt i pavarur publik (agjenci, qendër) i krijuar me akt të veçantë, me buxhetin e vet dhe mandatin e përcaktuar qartë. Qendra është e pavarur në punën e saj analitike, por është përgjegjëse për koordinimin me institucionet përkatëse përmes mekanizmave të formalizuar (memorandumet, rregulloret). Komiteti mbikëqyrës ose këshillimor siguron transparencë dhe pajtueshmëri me strategjitë kombëtare.

Funksionet kryesore:

- Monitorimi dhe Analiza Kombëtare e Mjedisit të Informacionit (NHMI), duke përfshirë tendencat, narrativat dhe teknikat;
- Koordinimi i institucioneve përmes një rrjeti të pikave të kontaktit dhe informimeve të rregullta;
- Standardet për shkëmbimin e informacionit dhe depon qendrore (formatet, metadatat, nivelet e konfidencialitetit);
- Katalogu dhe zbatimi i trajnimeve (bazë – të avancuar – të specializuara);
- Mbështetje për komunikimin institucional (zbulimi i hershëm i kërcënimeve (*prebunking*) dhe zbulimi i incidentit (*debunking*), pyetje dhe përgjigje, lista me fakte);
- Logjika e monitorimit dhe vlerësimit (treguesit e performancës, raportet tremujore dhe vjetore).

Procese dhe procedura standarde të operimit

Qendra miraton një "grup minimal" të procedurave standarde të funksionimit: raport-vlerësim-përgjigje (me afate kohore), matricë të vendimmarrësve, nivele të alarmit dhe shabllone të situatës (zgjedhje, kriza, ngjarje të ndjeshme). Është ndërtuar një cikël i përmbledhjeve të rregullta të situatës (mujore) dhe shënimeve analitike tematike.

Burimet dhe personeli

Bërthama e 15–25 profesionistëve (OSINT/Data Analytics, Cyber/Technical Profiles, Strategic Communications, Regulatory Affairs Lawyer, Monitoring and Evaluation). Një grup qendror mjete për monitorim dhe analitikë, me licenca të përbashkëta dhe mbështetje teknike.

Marrëdhëniet me publikun dhe komunikimi

Nuk është një qendër për demante, por një shërbim për bartësit e mesazheve (ministritë dhe agjencitë): përgatit rekomandime komunikimi, koordinon mesazhet parandaluese para periudhave të ndjeshme dhe siguron materiale për aplikim të menjëhershëm.

Bashkëpunim ndërkombëtar

Kontakti zyrtar me mekanizmat evropianë (p.sh. RAS) dhe me qendrat tematike (p.sh. Hybrid CoE), pjesëmarrja në trajnime dhe ushtrime simulimi dhe ndarja e standardeve.

Përparësitë

Identitet i qartë institucional; ekspertizë dhe mjete të centralizuara; kujtesë e qëndrueshme institucionale; llogaridhënie dhe shikueshmëri e lartë.

Kufizimet

Nevoja për një kornizë dhe buxhet të ri ligjor; rreziku i dublikimit nëse rolet nuk specifikohen; koha e nevojshme për personelin dhe procedurat.

4.2. Opsioni B: Mekanizmi Kombëtar i Koordinimit në kuadër të Qeverisë

Organizimi i menaxhimit

Zyra koordinuese e integruar në Qeveri (nën Kryeministrin, sekretariatin e përgjithshëm, etj.), e cila funksionon si një "bërthamë + rrjet". Bërthama koordinon ndërsa resorët miratojnë dhe zbatojnë. Vertikalja politike lejon përshkallëzim të shpejtë dhe sinkronizim midis ministrive dhe agjencive.

Funksionet kryesore

- Organizimi i njoftimeve mujore të situatës dhe vlerësimet tremujore të rrezikut (probabiliteti x ndikimi). Kornizat PMESII dhe AIC janë praktike për strukturimin e

vlerësimeve (US Army, 2015);

- Model standard i dakordësuar për raportimin dhe ndjekjen e incidenteve dhe depo ndërdepartamentale (teknikisht mund të organizohet nga një institucion ekzistues);
- Harmonizimi i komunikimit publik (udhëzime, pyetje dhe përgjigje, lista me fakte);
- Koordinimi i katalogut të trajnimeve (zbatimi përmes resorëve dhe partnerëve);
- Ndërlidhja me mekanizmat e NATO-s dhe BE-së.

Procese dhe procedura standarde të operimit

Baza janë procedurat operative standarde "të thjeshta, por të detyrueshme" për vlerësimin-përgjigje: hapa dhe afate kohore të qarta; matrica e bartësve; shkalla e përshkallëzimit (kush-kujt-kur). Kalendari i brendshëm krijon një ritëm (mujor në nivel teknik, tremujor në një nivel më të lartë).

Burimet dhe personeli

Bërthama numëron 8-12 persona (koordinatorë, analistë, specialistë të komunikimit, avokatë dhe koordinatorë të monitorimit dhe vlerësimit). Mjetet e monitorimit dhe analizës sigurohen përmes marrëveshjeve kornizë dhe licencave dhe përdoren përmes platformave dhe kapaciteteve ekzistuese të institucioneve, pa dublikim të infrastrukturës.

Marrëdhëniet me publikun dhe komunikimi

Koordinimi i mesazhit është një veçori mbështetëse: udhëzimet e harmonizuara të komunikimit, një kalendar i folësve të autorizuar dhe përmbledhje të shkurtra parandaluese para temave të ndjeshme. Vizibiliteti publik është i moderuar, pasi theksi kryesor është në koordinimin e brendshëm në kohë dhe sigurimin e listave me fakte, pyetje dhe përgjigje që portofolet mund t'i përdorin menjëherë. Kanalet në internet mundësojnë 'veprim lidhës' dhe mobilizim të shpejtë të audiencës (Bennett & Segerberg, 2012).

Bashkëpunim ndërkombëtar

Zyra Qeveritare vepron si një pikë e vetme kontakti me RAS, EEAS dhe qeveritë partnere, duke mundësuar shkëmbimin e shpejtë dhe formal të informacionit, pjesëmarrjen në kohë në paralajmërime dhe përfshirjen në analiza dhe ushtrime të përbashkëta.

Përparësitë

Fillim i shpejtë pa një institucion të ri; peshë e fortë ndër-departamentale; gjurmë minimale institucionale; përafrim i lehtë me burimet ekzistuese.

Kufizimet

Varësia nga stabiliteti i udhëheqjes politike dhe prioriteteve; rreziku që thellësia analitike të jetë e kufizuar nëse bërthama është shumë e vogël; dukshmëria për publikun dhe akademinë mund të jetë më e ulët.

4.3. Opsioni C: Forcimi i Këshillit ekzistues për Koordinim të Komunitetit të Inteligjencës së Sigurisë

Organizimi i menaxhimit

Ngritja e Këshillit ekzistues për Koordinim të Komunitetit të Inteligjencës së Sigurisë, me mandat të shtuar qartë për NHMI-në. Krijohet "bërthama e sekretariatit" që siguron procese, dokumentacion dhe mbështetje analitike dhe portofolet mbeten transportuesit kryesorë.

Funksionet kryesore

- Kalendari i takimeve rutinë (mujor në nivel teknik, tremujor në nivel menaxherial);
- Miratimi i procedurave standarde të operimit me skenarë, lista kontrolli dhe kanale të qarta përshkallëzimi;
- Depoja e përbashkët dhe formati standard për incidentet dhe analizat;
- Linja e komunikimit të brendshëm: rruga e qartë "kush shkruan - kush kontrollon - kush miraton - kush publikon", me modele pyetjesh dhe përgjigjesh dhe zëdhënës të emëruar, dhe nëse është e nevojshme koordinon me bartësit e resorëve;
- Përfshirja në mekanizmat evropianë përmes pikave të emërtuara të kontaktit.

Procese dhe procedura standarde të operimit

Fokusi është në "ringjalljen" e koordinimit: informime të rregullta, vendime të dokumentuara dhe ndjekje të realizimeve. Rutinat dhe "organizimi i kujdesshëm" rrisin sigurinë organizative dhe rezistencën (Weick & Sutcliffe, 2007). Procedurat standarde të funksionimit duhet të jenë specifike (kush, çfarë, kur), me tregues të shkurtër të statusit.

Burimet dhe personeli

Bërthama e sekretariatit prej 5-8 personash me kompetencë procesi dhe analitike, rrjeti i pikave të kontaktit në institucionet përkatëse dhe përdorimi i mjeteve dhe infrastrukturës

ekzistuese pa dublikim. Investimi në kapacitetet, proceset dhe infrastrukturën njerëzore është një parakusht për qëndrueshmërinë (UNDP, 2021).

Marrëdhëniet me publikun dhe komunikimi

Këshilli tradicionalisht funksionon si një organ koordinues i brendshëm ndërsa komunikimi publik realizohet përmes institucioneve përkatëse. Nevojiten rregulla të qarta kur dhe si të dalin me mesazhe të harmonizuara dhe kush është folës i autorizuar në situata specifike. Transparenca më e madhe shoqërohet me besim më të lartë në institucione (Grimmelikhuijsen et al., 2013).

Bashkëpunim ndërkombëtar

Kontaktet me partnerët e jashtëm mbahen përmes resorëve dhe përmes pikave të emërtuara të kontaktit, dhe Sekretariati koordinon dokumentet, formatet dhe afatet.

Përparësitë

Kostoja më e ulët institucionale; shfrytëzimi i arkitekturës ekzistuese dhe kanaleve të besuara; operacionalizimi relativisht i shpejtë.

Kufizimet

Vizibilitet më i ulët publik; rreziku që koordinimi të mbetet formal pa zbatim real; varësia nga disiplina dhe udhëheqja e qëndrueshme në Këshill.

Tabela 5: Opsionet për arkitekturat për reagimin sistematik ndaj NHMI-së

Kriteri	Opsioni A: Qendër e pavarur	Opsioni B: Mekanizëm koordinimi në kuadër të Qeverisë	Opsioni C: Këshilli i Forcuar i Koordinimit të Komunitetit të Inteligjencës dhe Sigurisë
Organizimi i menaxhimit	Subjekt i pavarur publik (agjenci/qendër) me buxhetin e vet dhe komisionin mbikëqyrës/ këshillimor.	Zyra koordinuese në kuadër të Kryeministrit/ Sekretariatit të Përgjith-shëm ("core + network").	Këshilli ekzistues me bazë sekretariati dhe mandat të zgjatur.

Kriteri	Opsioni A: Qendër e pavarur	Opsioni B: Mekanizëm koordinimi në kuadër të Qeverisë	Opsioni C: Këshilli i Forcuar i Koordinimit të Komunitetit të Inteligjencës dhe Sigurisë
Mandati dhe funksionet	Monitorimi dhe analiza e NHMI-së; koordinimi përmes pikave të fokusit; standardet dhe depoja; trajnimet; mbështetja e komunikimit; monitorimi dhe vlerësimi; marrëdhëniet BE/NATO.	Koordinimi rutinor; njoftimet mujore dhe vlerësimet tremujore; shablloni dhe ndarja standarde; komunikimi i harmonizuar publik; katalogu i trajnimeve; lidhjet BE/NATO.	Takimet e rregullta (niveli teknik/menaxherial); procedurat standarde operative me skenarë; depo e përbashkët; linjat e brendshme të komunikimit; kontaktet e BE-së përmes pikave qendrore.
Proceset / PSO-të	Procedurat standarde të formalizuara të funksionimit (raport-vlerësim-përgjigje); nivelet e alarmit; shabllonet për situatat; informimet mujore.	Procedurat standarde të funksionimit "të lehta", por të detyrueshme; kalendari (mujor/tremujor); kanalet e përshkallëzimit.	Rigjallërimi i koordinimit: listat kontrolluese specifike të procedurave standarde të funksionimit; vendimet e dokumentuara dhe ndjekja.
Stafi (pika referimi)	Bërthama 15–25 (OSINT/ analitikë, kibernetikë/ teknikë, komunikime, ligj, monitorim dhe vlerësim).	Bërthama 8–12 (koordinimi, analitika, komunikimet, ligji, monitorimi dhe vlerësimi).	Sekretariati 5–8 + pikat e kontaktit në institucione.
Mjetet/ Depoja	Një grup qendror mjetesh dhe një depo kombëtare pritëse me standarde për metadata.	Qasje e koordinuar (marrëveshje/licenca kornizë); depo e organizuar në një institucion ekzistues.	Përdorimi i mjeteve ekzistuese; depoja dhe formati i rënë dakord.
Komunikimi me publikun	Përgatit rekomandime/ materiale të gatshme për përdorim; mbështet bartësit e mesazheve.	Harmonizon mesazhe dhe orarin e bartësve; dukshmërinë mesatare të publikut.	Kryesisht koordinimin e brendshëm; komunikimin publik përmes resorëve.
Bashkëpunim ndërkombëtar	Ndërfaqe formale me mekanizmat e BE-së dhe NATO-s; pjesëmarrje në trajnime dhe ushtrime të specializuara.	Ndërfaqe natyrore e qeverisë me mekanizmat e BE-së/NATO-s; komunikimi i shpejtë formal.	Kontaktet përmes resorëve dhe pikave të emërtuara; koordinimi përmes sekretariatit.
Përparësitë (përmbledhje)	Identitet i qartë; ekspertizë e centralizuar; stabilitet dhe llogaridhënie e lartë.	Fillim i shpejtë; peshë e fortë ndër-resoriale; gjurmë minimale institucionale.	Kostoja më e ulët institucionale; përdor kanalet ekzistuese; operacionalizimi i shpejtë.

Kriteri	Opsioni A: Qendër e pavarur	Opsioni B: Mekanizëm koordinimi në kuadër të Qeverisë	Opsioni C: Këshilli i Forcuar i Koordinimit të Komunitetit të Inteligjencës dhe Sigurisë
Kufizimet (përmbledhje)	Kornizat e reja ligjore/ buxhetore dhe diferencimi i roleve të nevojshme.	Varësia nga vazhdimësia politike; rreziku i analizave të cekëta nëse bërthama është "e hollë".	Inercia historike; dukshmëria e ulët publike; suksesi varet nga disiplina.
Koha e funksionimit	Afati më i gjatë i përdorimit (kërkohet projektimi dhe formimi para fillimit).	Afatshkurtër (në mënyrë operative për disa muaj).	Afatshkurtër (reforma e ekzistueses dhe krijimi i rutinave).



KAPITULLI 5:

PËRFUNDIM DHE REKOMANDIME PËR ZBATIM

5.1. Vërejtje përfundimtare

Maqedonia e Veriut, si një vend me pozicion strategjik gjeopolitik, anëtar i NATO-s dhe me ambicie të shprehura qartë për integrimin në BE, është në një pikë ku duhet të zhvillojë përgjigjen kombëtare ndaj ndërhyrjes së huaj dhe manipulimit të informacionit brenda një kornize gjithëpërfshirëse dhe të koordinuar. Ndërtimi i qëndrueshmërisë sociale dhe institucionale nuk mund të arrihet me aktivitete të izoluara, por duke krijuar një sistem të integruar të bazuar në promovimin strategjik, koordinimin institucional, arsimin, ndërgjegjësimin e publikut dhe bashkëpunimin ndërkombëtar.

Nevojitet një **rishikim dhe përmirësim i Strategjisë Kombëtare për Rezistencën ndaj Kërcënimeve Hibride**, e cila duhet të bazohet në analiza moderne dhe tipologji të reja të kërcënimeve, të tilla si operacionet njohëse dhe ndikimi algoritmik. Strategjia duhet të jetë një dokument i gjallë që përshtatet me ndryshimin e mjedisit të sigurisë përmes një mekanizmi të integruar monitorimi dhe vlerësimi, i cili do të mundësojë përshtatjen dinamike të politikave. Përveç kësaj, ndërhyrja ligjore është thelbësore. **Përcaktimi ligjor i NHMI-së** është parakusht për një koordinim dhe llogaridhënie institucionale efektive. Për të mundësuar vendimmarrje të informuar, është e nevojshme të krijohen **mjete vlerësimi** që do të përdorin modele të zbatueshme për analizën e kërcënimeve hibride dhe vlerësimin e rrezikut në mjedisin operacional.

Qëndrueshmëria ndaj NHMI-së varet nga **ekzistenca e një mekanizmi kombëtar të koordinimit**, i cili do të mundësojë shkëmbimin e rregullt të informacionit, vlerësimin e përbashkët dhe përgjigjen e harmonizuar. Për të arritur këtë, është e nevojshme të **forcohen kapacitetet institucionale** duke investuar në burimet njerëzore, infrastrukturën digjitale dhe teknologjitë analitike. Në të njëjtën kohë, shteti duhet të ndërtojë **kujtesën institucionale**, domethënë një sistem për arkivimin, analizimin dhe mësimin nga rastet e mëparshme, i cili do të parandalojë përsëritjen e mosveprimeve dhe do të rrisë parandalimin. **Përfshirja e shoqërisë civile, akademisë dhe mediave** në procese do të mundësojë krijimin e një sistemi më transparent, gjithëpërfshirës dhe të qëndrueshëm të rezistencës.

Edukimi dhe arsimimi mediatik gjithashtu luajnë një rol qendror në ndërtimin e një shoqërie rezistente. Është e nevojshme të promovohen programet kombëtare të edukimit mediatik dhe digjital që do të mbulojnë të gjitha kategoritë e moshave dhe do të integrohen në arsimin formal dhe joformal. Përveç kësaj, trajnimet e specializuara për administratën publike dhe profesionistët e medias janë të nevojshme për të forcuar kapacitetet për njohjen, analizimin dhe reagimin e duhur ndaj manipulimeve të informacionit.

Ndërtimi i qëndrueshmërisë shoqërore kërkon gjithashtu përfshirjen e qytetarëve. **Fushatat sistematike të informimit dhe edukimit** janë një mjet kryesor për të forcuar mendimin kritik dhe njohjen e dezinformatave. Në këtë proces, **komunikimi institucional transparent dhe i përgjegjshëm** është themeli i besimit midis institucioneve dhe qytetarëve.

Së fundi, **bashkëpunimi rajonal dhe ndërkombëtar** është parakusht për një përgjigje efektive ndaj NHMI-së. Për njohjen dhe neutralizimin në kohë të ndikimeve të huaja, është

veçanërisht e rëndësishme, **për integrimin në mekanizmat evropianë** Seti i mjeteve për përgjigje ndaj NHMI-së (*FIMI Toolbox*) dhe Sistemin për Alarmim të Shpejtë (*Rapid Alert System - RAS)*, i zhvilluar nga Shërbimi Evropian për Veprim të Jashtëm (EEAS), është veçanërisht i rëndësishëm.

5.2. Rekomandime për zbatimin

Që Maqedonia e Veriut të transformojë arkitekturën e saj institucionale për një përgjigje të integruar që jo vetëm i përgjigjet kërcënimeve, por i parashikon, analizon dhe parandalon ato, ky dokument politikash rekomandon **tre opsione politikash: (1) Qendra e Pavarur për Qëndrueshmëri Kombëtare, (2) Mekanizmi Kombëtar i Koordinimit nën Qeverinë, ose (3) Këshilli i Forcuar i Koordinimit të Komunitetit të Inteligjencës dhe Sigurisë**. Qasja parashikon një ndërtim të qëndrueshëm të rutinave që do të mbeten pas ndryshimit të udhëheqjes dhe prioriteteve, dhe synimi është që sistemi të funksionojë në rrethana të zakonshme, jo vetëm në një krizë.

Pavarësisht nga zgjedhja e modelit institucional, ky dokument ofron **rekomandimet ose udhërrëfyesin e mëposhtëm për zbatim**:

- **Të sigurohet një bartës i qartë i procesit dhe legjitimitet formal**. Nëse do të jetë një qendër autonome, një mekanizëm koordinimi qeveritar ose një këshill i forcuar, mandati duhet të përshkruhet qartë me pak fjalë: me objektiva, fushëveprim, përgjegjësi dhe kanale dhe rregulla të qarta për bashkëpunim me institucionet kryesore.

- Çdo institucion përkatës duhet të emërojë një pikë fokale dhe një zëvendës, me një faqe përshkrimi të rolit, hapat kur dhe kujt i përcillet çështja dhe detyrimet për raportim të rregullt.

- **Vendosja e një kalendari të rutinave** pasi të krijohet kjo infrastrukturë minimale, përkatësisht: takime të shkurtra teknike me një situatë të shkurtër një herë në muaj dhe më shumë takime kompakte në një nivel më të lartë një herë në tremujor, në të cilat jepen udhëzime, ndiqen zgjidhje dhe kursi korrigjohet kur është e nevojshme. Për të mos humbur asgjë në shpejtësinë operacionale, një procesverbal i shkurtër i vendimeve për atë që është vendosur, kush është përgjegjës dhe çfarë vjen më pas përgatitet pas çdo takimi.

- **Të përcaktohet procedura kryesore e "raportimit-vlerësimit-përgjigjes"** . Ai përcaktohet nga një dokument i qartë që thotë: çfarë informacioni raportohet, në çfarë formati minimal, kujt i dorëzohet dhe brenda cilit afat; si kryhet një vlerësim i rrezikut (matricë e thjeshtë: probabiliteti x ndikimi); dhe si merret një vendim përgjigjeje, me përgjegjësi dhe pragje kohore të përcaktuara qartë. Kjo logjikë plotësohet nga disa skenarë universalë (periudha e zgjedhjeve, situatat e krizës, ngjarjet e ndjeshme), për të cilat paraprakisht përgatiten listat e kontrollit, transportuesit dhe formati i materialeve dalëse. Përkufizimi i qartë se kur dhe kujt i përcillet çështja ngrihet në një nivel më të lartë. Një faqe përcakton: kush vendos në nivel teknik, kur është i përfshirë transportuesi politik dhe në çfarë pike

informohet publiku. Këto pragje e bëjnë procedurën të parashikueshme dhe të barabartë.

- **Të zhvillohen kompetencat institucionale**. Në «bërthamën» e sistemit nevojiten të paktën tre lloje profilesh: analitikë dhe burime të hapura (me njohuri për të dhënat), lidhje TIK/kibernetike me aftësinë për të përkthyer një sinjal teknik në një mesazh të kuptueshëm operacional dhe komunikim strategjik për të formuluar materiale komunikimi të sakta, të qarta dhe konfidenciale. Kjo pasohet nga mbështetja ligjore për çështjet rregullatore dhe koordinimi për monitorim dhe vlerësim, edhe nëse disa nga këto role janë të përbashkëta. Ky profil i personelit ka kuptim vetëm nëse mbështetet nga një grup i përbashkët mjetesh monitorimi dhe analize dhe nga një infrastrukturë e thjeshtë dhe e fuqishme për regjistrimin e rasteve.

- **Të krijohet katalog për trajnime** në tre nivele: module bazë për të gjitha pikat e fokusit, të avancuara për analistët dhe komunikuesit dhe të specializuara për skenarët zgjedhorë dhe të krizave. Çdo trajnim duhet të ketë një qëllim të qartë, afat kohor dhe rezultat të dukshëm (mjet ose dokument për përdorim), me një certifikatë zyrtare për trajnim të përfunduar që do të ruajë kujtesën institucionale edhe gjatë rotacioneve të stafit.

- **Të përgatiten mesazhe të shkurtra dhe të kuptueshme për narrativat e pritshme** edhe para se të shfaqen në periudha të ndjeshme. Në vend që të pritet demant, komunikimi me publikun meriton trajtim të veçantë, parandalues. Këto shpjegime për zbulimin paraprak të kërcënimeve (*prebunking*) nuk janë propagandë, por një shërbim për qytetarët: çfarë është fakt, çfarë është spekulim dhe ku të kontrollohen informacionet. Kur korrigjimi është i nevojshëm, përdoret një format standard i pyetjeve dhe përgjigjeve dhe fletëve me fakte që mund të merren shpejt nga institucionet bartëse. Rregulli i ekspozimit «minimal i nevojshëm» është i rëndësishëm: publiku duhet të informohet, por pa amplifikim të panevojshëm të narrativave manipuluese. Që kjo të funksionojë, duhet të ketë një listë të azhurnuar të kontakteve dhe një protokoll të qartë për të punuar me mediat dhe platformat, me udhëzime për transparencë dhe koordinim kohor.

- **Të standardizohet shkëmbimi i informacioneve** për të zvogëluar zhurmën dhe për të shpejtuar vendimet. Çdo incident ose vëzhgim përkatës regjistrohet me një grup minimal por të detyrueshëm fushash: data dhe koha, burimi ose lidhja, përshkrimi i shkurtër, vlerësimi i probabilitetit dhe ndikimit, masat e marra dhe statusi aktual. Këto regjistrime ruhen në një vend të përbashkët, të kontrolluar, me versionim dhe meta-data themelore; nuk është vendimtare se ku ndodhet depoja, por të jenë të qëndrueshme, të qëndrueshme dhe të kenë nivele të qarta të qasjes. Kur rasti ka një dimension ndërkufitar, protokolli i brendshëm duhet të specifikojë se kush dhe kur fillon aktivizimin e kanaleve evropiane, në veçanti Sistemin për Alarmim të Shpejtë (*RAS*), duke e bërë kështu përpjekjen kombëtare pjesë të një koordinimi më të gjerë.

- **Të vendoset një matje minimale** që sistemi të mësojë. Nuk ka nevojë për korniza komplekse treguese; mjafton një grup i vogël treguesish në çdo fushë: rregullsia dhe cilësia e informimeve dhe takimeve; numri dhe mbulimi i pikave fokale të trajnuara; koha nga sinjali deri në mesazhin e parë të koordinuar; shtrirja dhe kuptueshmëria e komunikimeve;

dhe përqindja e hyrjeve që mbërrijnë në një format standard. Këta tregues janë konsoliduar në një përmbledhje të shkurtër mujore të situatës dhe një rishikim tremujor në të cilin ka gjithmonë vend për dy ose tre masa specifike korrigjuese. Krijimi i një sistemi të mësimeve të nxjerra ushqen kujtesën institucionale dhe zvogëlon varësinë nga individët.

Ky udhërrëfyes përcakton infrastrukturën minimale, por kryesore: një transportues të qartë, një rrjet pikash kontakti, procedura praktike, kompetenca thelbësore, komunikim parashikues dhe matshmëri që nxit të mësuarit. Kështu, pavarësisht nëse zgjidhet një qendër e pavarur, një mekanizëm koordinimi qeveritar ose një këshill i reformuar, sistemi merr një «ritëm» që e kthen qëllimin e mirë në praktikë të përditshme.

PËR AUTORËT

Dr. Aleksandar Grizhev është profesor i asociuar në Akademinë Ushtarake "Gjeneral Mihailo Apostolski" – Shkup dhe shef i Katedrës së Shkencave Sociale dhe Humane. Fokusi i tij mësimor dhe kërkimor është në studimet e mbrojtjes së sigurisë, stabilizimin dhe rindërtimin pas konfliktit, reformën e sektorit të sigurisë (*SSR*), radikalizimin dhe ekstremizmin e dhunshëm, operacionet kognitive dhe perspektivën gjinore në forcat e armatosura dhe sektorin e gjerë të sigurisë. Ai ka përvojë operacionale nga misionet ndërkombëtare, duke përfshirë pjesëmarrjen në Misionin Special të Monitorimit të OSBE-së në Ukrainë (2019–2021), si dhe angazhimet e mëparshme në mjedise konflikti dhe pas konfliktit. Ai merr pjesë rregullisht në forume ndërkombëtare dhe është pjesë e projekteve dhe aktiviteteve të ndryshme me partnerë kombëtarë dhe ndërkombëtarë (*NATO Science and Technology Organization, NATO Committee on Gender Perspective, OSCE, UN, RACVIAC, PfP Consortium*). Me një interes të veçantë në dimensionet kulturore dhe fetare në operacione, ai eksploron ndërtimin e rezistencës institucionale ndaj kërcënimeve hibride, me një fokus të veçantë në ndërhyrjen e huaj dhe manipulimin e informacionit (NHMI), koordinimin institucional, rezistencën e publikut ndaj narrativave manipuluese dhe komunikimit etik në sektorin e sigurisë.

Dr. Vesna Poposka është profesoreshë universitare, analiste e pavarur dhe e vetmja grua me doktoraturë të mbrojtur në Akademinë Ushtarake "Gjeneral Mihailo Apostolski" në Shkup - një arritje që e pozicionon atë si pioniere në studimet e sigurisë dhe mbrojtjes në Maqedoninë e Veriut. Ekspertiza e saj mbulon çështje në fushën e sigurisë kombëtare, kërcënimeve hibride, qëndrueshmërisë demokratike dhe kuadrit ligjor të politikave të mbrojtjes. Poposka ka marrë pjesë në Shkollën e Këshillit të Evropës për Politikë, Shkollën Presidenciale për Liderë të Rinj dhe Forumin e Sigurisë në Varshavë - tre platforma prestigjioze që formësojnë perspektivën e saj strategjike dhe e lidhin atë me rrjetet kryesore evropiane dhe globale të sigurisë. Ajo është hulumtuese e jashtme në Institutin e Prespës, ku punon në projekte që lidhen me demokracinë, të drejtat e njeriut dhe stabilitetin rajonal, me theks të veçantë në rezistencën e institucioneve ndaj ndikimeve hibride. Si profesoreshë e asocuar në Akademinë Ushtarake në Shkup, ajo kontribuon në mënyrë aktive në zhvillimin e kurrikulave moderne në fushën e sigurisë dhe mbrojtjes, me fokus në kërcënimet hibride, komunikimin strategjik dhe ndërtimin e qëndrueshmërisë institucionale. Angazhimi i saj akademik pasohet nga paraqitje të shumta publike, panele diskutimesh dhe publikime. Vesna Poposka është një mbështetëse e zëshme e barazisë gjinore në sektorin e sigurisë dhe avokon për përfshirje më të madhe të grave në proceset e vendimmarrjes dhe politikëbërjes.

LITERATURA E PËRDORUR

- Banas, J. A. & Miller, G., 2013. *Inducing resistance to conspiracy theory propaganda: Testing inoculation and metainoculation strategies. Human Communication Research*, 39(2), pp.184–207.
- Bennett, W.L. & Segerberg, A., 2012. The logic of connective action. Information, Communication & Society, 15(5), pp.739–768.
- Blair-Simon, K. (2025). Ndërhyrja e huaj dhe manipulimi me informacionet në kontekstin e rregulloreve evropiane. Instituti për Studime të Komunikimit. ResPublica, Shkup.
- Bryman, A. (2016) Social Research Methods. 5th edn. Oksford: Oxford University Press. Qeveria e Republikës së Maqedonisë së Veriut (2021).
- Center for Democratic Transition (CDT) (2024). *Foreign Influences on the Electoral Process in Montenegro 2016–2023*. Podgoricë: CDT. Në dispozicion në: https://en.cdtmn.org/wp-content/uploads/2024/05/CDT-Foreign-Influences-on-the-Electoral-Process-in-Montenegro-2016%E2%80%932023.pdf
- European Commission, 2020. *Action Plan Against Disinformation*. Brussels.
- European Commission (2023) *Flash Eurobarometer 528: Citizenship and Democracy.* Fieldwork: April–May 2023; Published: 6 December 2023. Luxembourg: Publications Office of the EU.
- European External Action Service – EEAS (2023). *1st EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats. Towards a framework for networked defence. Brussels: EEAS.*
- European External Action Service – EEAS (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence.*
- European External Action Service (2025) *Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI).*
- EU StratCom Task Force, 2022. *FIMI Toolbox Overview.*
- Grimmelikhuijsen, S.G. et al., 2013. *The effect of transparency on trust in government: A cross-national comparative experiment. Public Administration Review*, 73(4), pp.575–586.
- Haxhi-Janev, M. Dhe Stoilkovski, M. (2025). Ndërhyrja e huaj dhe manipulimi me informacionet në Republikën e Maqedonisë së Veriut: Analiza fillestare. Shkup: Instituti për Studime të Komunikimit. ResPublica. Shkup.
- Hoffman, F.G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies.
- House of Commons Library (2024). *Romania: recent political developments and 2024 elections* (CBP-10164), 23 December. London: UK Parliament. Në dispozicion në: https://commonslibrary.parliament.uk/research-briefings/cbp-10164/?utm_source=chatgpt.com

- Instituti Ndërkombëtar Republikan (2024). Sondazhi Rajonal i Ballkanit Perëndimor, 2 Shkurt–Mars
- IREX (2023) *Vibrant Information Barometer 2023: Montenegro*. Washington, DC: IREX. Në dispozicion në:https://www.irex.org/files/vibrant-information-barometer-2023-montenegro.pdf?utm_source=chatgpt.com
- Keohane, R.O. & Nye, JS, 1998. *Power and Interdependence in the Information Age*. Foreign Affairs, *77*(5), pp.81–94.
- Livingstone, S. & Helsper, E.J., 2007. *Gradations in digital inclusion: Children, young people and the digital divide*. New Media & Society, 9(4), fq.671-696.
- Misioni i BE-së për Vëzhgimin e Zgjedhjeve (2025). *Deklarata Paraprake - Zgjedhjet Parlamentare, Kosovë, 9 shkurt 2025*. Prishtinë: EU EOM, 11 shkurt Në dispozicion në: https://www.eods.eu/library/EU%20EOM%20Kosovo%202025_Preliminary%20Statement_ENG.pdf
- Mozilla Foundation (2024). *Election Manipulation in Brazil's 2022 General Elections: The Role of WhatsApp and Telegram on the Attacks Against Electoral Integrity*. 27 shkurt. Në dispozicion në: https://www.mozillafoundation.org/en/research/library/global-elections-casebook/brazil-case-study/
- NATO, 2020. *Countering Hybrid Threats*. NATO Review.
- OECD, 2017. *Evaluating Development Activities: 12 Lessons from the OECD DAC*. Paris.
- Pamment, J., 2020. *Resilience to Foreign Information Manipulation: The Role of Strategic Communication*. Carnegie Endowment.
- Popovska V. (2024). Mbrojtja e informuar – Hyrje në kërcënimet hibride në infrastrukturën kritike. Instituti PRESPA – Shkup. Në dispozicion në: http://www.prespa-institute.mk/wp-content/uploads/2024/02/Informirana-odbrana.pdf
- Reuters (2025). *'Does Musk's interview with German AfD leader square with EU laws?'*, 9 January. Në dispozicion në: https://www.reuters.com/world/europe/how-musks-interview-with-german-afd-leader-squares-with-eu-laws-2025-01-09/
- Rid, T., 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
- Strategjia Kombëtare për Ndërtimin e Rezistencës dhe Ballafaqimin me Kërcënimet Hibride 2021–2025 (me Planin e Veprimit). Shkup.
- UNDP, 2021. *Institutional Capacity Assessment Framework*.
- US Army, 2015. *Operational Environment Assessment: PMESII-PT*.
- Wardle, C. & Derakhshan, H., 2017. *Information Disorder: Toward a Interdisciplinary Framework*. Council of Europe.
- Weick, K.E. & Sutcliffe, K.M., 2007. *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. Wiley.

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

342.5:[316.776.23:327.8(497.7)(047.31)

GRIZHEV, Aleksandar
Reagimi institucional ndaj nddrhyrjes sd huaj dhe manipulimit me informacionet në Maqedoninë eVeriut [Електронски извор] : modelet dhe opsionet për politika : dokument për politika publike / [autorë Aleksandar Grizhev, Vesna Poposka ; përkthim nga maqedonisht në shqip Vjosa Taipi]. - Shkup : Instituti për studime të komunikimit, 2025. - (Edicioni ResPublica)

Начин на пристапување (URL):
https://respublica.edu.mk/wp-content/uploads/2025/11/reagimi-institucional_fimi_al.pdf.
- Текст во PDF формат, содржи 54 стр. - Превод на делото: Институционален одговор на странското мешање и манипулирање со информации во Северна Македонија : модели и опции за политика : документ за јавна политика. - Наслов преземен од екранот. - Опис на изворот на ден 05.12.2025. - Për autorët: стр. 52. - Библиографија: стр. 53-54

ISBN 978-608-4805-67-0

1. Poposka, Vesna [автор]
а) Дезинформации -- Странски влијанија -- Институционален одговор -- Македонија -- Истражувања

COBISS.MK-ID 67704069

Институт за комуникациски студии
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 "Monitorimi, zbulimi dhe ekspozimi i ndërhyrjeve të fshehta të huaja dhe manipulimit të informacionit", 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.