Институт за комуникациски студии

Udhëzime:
Reagimi i qeverisë ndaj Ndërhyrjes së Huaj dhe Manipulimit të Informacionit (NHMI) në Maqedoninë e Veriut



Ky udhëzim i ofron qeverisë së Maqedonisë së Veriut një kornizë strategjike për adresimin e Ndërhyrjes së Huaj dhe Manipulimit të Informacionit (NHMI). Objektivi kryesor është ndërtimi i një shoqërie më rezistente ndaj dezinformatave me kalimin e kohës, duke mbrojtur njëkohësisht sigurinë kombëtare dhe lirinë e shprehjes. Për të siguruar që kjo kornizë të mbetet efektive, qeveria duhet të angazhohet për hetimin e vazhdueshëm të operacioneve të NHMI-së, duke përdorur mësimet e nxjerra nga ndërhyrjet e mëparshme për të përmirësuar dhe forcuar vazhdimisht masat e saj mbrojtëse.

Seksioni 1: Pse NHMI-ja është një kërcënim kombëtar

Për të mbrojtur shoqërinë, qeveria duhet ta përcaktojë NHMI-në si një kërcënim për sigurinë kombëtare. Për ta bërë këtë në mënyrë efektive, duhet të shpjegohen karakteristikat konkrete të NHMI-së, bazuar në operacionet e mëparshme që kanë shënjestruar si Maqedoninë e Veriut, ashtu edhe rajonin më të gjerë evropian. Duke analizuar këto modele të përsëritura, mund ta kategorizojmë rrezikun përmes katër këndvështrimeve të veçanta: burimit, mënyrës, objektivit dhe ndikimit.

1. Burimi

Është jetike të bëhet dallimi ndërmjet dezinformimit të brendshëm dhe ndërhyrjes ndërkombëtare. Ndërsa dezinformimi i brendshëm përhapet nga aktorë të brendshëm si politikanë lokalë ose influencues për përfitime brenda vendit, NHMI-ja drejtohet nga aktorë të lidhur me një shtet të huaj. NHMI-ja zakonisht qarkullon përmes një rrjeti kompleks të krijuar për të fshehur origjinën e saj të vërtetë.

- Kanale zyrtare shtetërore: Këto janë llogari të verifikuara të qeverive të huaja, si profile diplomatike në rrjetet sociale, të përdorura për të promovuar agjendat shtetërore.

- Media të kontrolluara nga shteti: Në vend që të jenë organizata të pavarura, këto funksionojnë si aparate propagandistike –-si RT dhe Sputnik - të cilat financohen nga shtete të huaja dhe nuk kanë pavarësi redaksionale.

- Kanale të fshehta të lidhura: Kjo përfshin një rrjet "hije" të influencuesve në rrjetet sociale, faqeve proxy dhe llogarive të automatizuara (bot), të cilat nuk i zbulojnë publikisht lidhjet e tyre të huaja, por përsërisin në mënyrë të saktë narrativat shtetërore.

2. Mënyra

NHMI-ja përcaktohet nga sjellja dhe metodat mashtruese të veprimit, dhe jo vetëm nga përmbajtja e mesazhit. Këto veprime janë të dizajnuara në mënyrë specifike për të mashtruar përdoruesit dhe për të manipuluar infrastrukturën teknike të platformave digjitale.

- Mimikria digjitale: Krijimi i ueb faqeve "klon" që duken identike me burime të besueshme të lajmeve për të mashtruar lexuesit, si operacioni Doppelgänger, i cili imitonte media të mëdha evropiane duke përfshirë Le Parisien dhe Le Figaro në Francë, Der Spiegel dhe Bild në Gjermani, La Stampa në Itali, Gazeta Wyborcza në Poloni dhe El Mundo në Spanjë.

- Aktivitet i koordinuar joautentik: Përdorimi i "fermave të bot-eve" për të postuar njëkohësisht të njëjtin mesazh, me qëllim mashtrimin e algoritmeve që një temë të bëhet

trend ose të përhapet dezinformim. Për shembull: Hetimi "Team Jorge" i kryer nga kolektivi investigativ Forbidden Stories zbuloi një paketë softuerike që u lejonte operatorëve të kontrollonin mbi 30,000 profile të sofistikuara dhe të verifikuara bot në platforma të ndryshme të rrjeteve sociale, me qëllim manipulimin e opinionit publik dhe zgjedhjeve në mbarë botën.

- Hakimi dhe publikimi (Hack-and-Leak): Vjedhja e informacionit privat dhe publikimi i tij në mënyrë strategjike për të dëmtuar reputacionin e një objektivi, një metodë që shpesh përdoret për të cenuar integritetin e zgjedhjeve. Për shembull: gjatë zgjedhjeve në SHBA në vitin 2016, emaile të vjedhura të fushatës u publikuan për të manipuluar opinionin publik.

- Deepfake: Përdorimi i inteligjencës artificiale për të krijuar video ose audio realiste, por të rreme, të udhëheqësve, me qëllim shkaktimin e konfuzionit ose panikut. Udhëheqësit botërorë dhe figurat politike shënjestrohen vazhdimisht nga deepfake-et në sulme dezinformuese

3. Objektivi

Objektivat e NHMI-së ndryshojnë në varësi të pozicionit të aktorit në rrjet, duke filluar nga strategjitë shtetërore në nivel të lartë deri te përfitimi në nivel të ulët.

- Përfitim politik: Qeveritë e huaja synojnë të destabilizojnë rivalët ose të ndikojnë në vendime të rëndësishme. Operacionet e NHMI-së intensifikohen gjatë momenteve kritike. Në Maqedoninë e Veriut: Në vitin 2018, dezinformimi u përdor për të minuar Marrëveshjen e Prespës – traktatin që zgjidhi një mosmarrëveshje të gjatë për emrin me Greqinë, duke mundësuar integrimin euro-atlantik. Në Rumani: Gjatë zgjedhjeve të vitit 2024, ndërhyrja e huaj përdori fushata të koordinuara me volum të lartë në rrjetet sociale për të manipuluar elektoratin.

- Përfitim financiar: Dezinformimi shpesh funksionon si një model biznesi, ku "sipërmarrës të vegjël" paguhen për klikime. Rasti i Velesit: Adoleshentë në Maqedoninë e Veriut prodhuan përmbajtje pro-Trump para zgjedhjeve në SHBA të vitit 2016, sepse gënjeshtrat sensacionaliste gjeneronin të ardhura të larta nga reklamat.

4. Ndikimi

Përtej ndikimit të menjëhershëm politik, ndikimi përfundimtar i NHMI-së është erozioni sistematik i "ngjitësit shoqëror" të një vendi. Duke e përmbytur mjedisin informativ me kontradikta, këto operacione nxisin një mosbesim të thellë që i çon qytetarët të vënë në dyshim edhe institucionet demokratike legjitime. Për më tepër, NHMI-ja përbën një kërcënim të drejtpërdrejtë për sigurinë publike; gjatë krizave si një pandemi ose emergjencë sigurie, dezinformimi i huaj mund të çorientojë publikun mbi protokollet e sigurisë, duke shkaktuar potencialisht trazira civile ose kriza të shëndetit publik.

Seksioni 2: Si të identifikohet NHMI-ja?

Identifikimi i NHMI-së kërkon një ndryshim në fokus. Në vend që të përpiqemi të monitorojmë ose kontrollojmë atë që njerëzit thonë, ne analizojmë taktikat, teknikat dhe procedurat specifike (TTP) që përdoren për të përhapur mesazhin. Duke e zbërthyer një operacion në këto tre shtresa, autoritetet mund të njohin ndërhyrjen e huaj edhe kur vetë përmbajtja nuk është e paligjshme.

1. Taktika (strategjia)

Taktikat janë „pse“ -ja e një operacioni. Ato janë qëllimet strategjike që një aktor i huaj synon të arrijë, si p.sh. “ndarja e opinionit publik” ose “dëmtimi i besimit në institucione”.

- Shembull: Gjatë negociatave për Marrëveshjen e Prespës, taktika strategjike ishte të minohej rruga e Maqedonisë së Veriut drejt BE-së dhe NATO-s duke krijuar ndarje të thella në shoqëri.

2. Teknikat (metoda)

Teknikat janë „truket“ ose metodat specifike të përdorura për të kryer një taktikë. Kjo shtresë përshkruan mënyrën se si aktori maskon identitetin e tij ose e shtyn mesazhin e tij përpara.

- Shembull: Mimikria digjitale është një teknikë e zakonshme ku aktorët krijojnë versione të rreme të faqeve të internetit të besueshme për ta bërë propagandën të duket si lajm i vërtetë.

3. Procedurat (ekzekutimi)

Procedurat janë pjesa më e detajuar e analizës. Ato janë veprimet teknike hap pas hapi dhe mjetet specifike të përdorura për të kryer operacionin. Kjo përfshin softuerin specifik, kohën e postimeve dhe konfigurimet teknike të nevojshme.

- Shembull: Përdorimi i një pakete softuerike për të menaxhuar mijëra profile të rreme njëkohësisht – siç u pa në hetimin Team Jorge - është një procedurë specifike për “sjellje të koordinuar joautentike”.

Duke dokumentuar këto modele, qeveria mund të krijojë një “manual” të ndërhyrjes. Kjo u lejon agjencive të sigurisë të identifikojnë një sulm bazuar në sinjale paralajmëruese (red flags), duke ofruar një arsye të qartë për të vepruar pa ndërhyrë në të drejtën ligjore të lirisë së shprehjes.

Seksioni 3: Si të trajtohet NHMI-ja?

Një përgjigje e suksesshme ndaj NHMI-së nuk qëndron vetëm në demaskimin e dezinformatave, pasi përfshirja me gënjeshtrat e huaja shpesh vetëm i përhap ato më tej. Meqenëse korrigjimet, si verifikimi i fakteve, jo gjithmonë arrijnë te të gjithë ose nuk i ndryshojnë mendimet e tyre, qeveria duhet të kalojë nga reagimi në qasje proaktive. Kjo nënkupton ndërtimin e një "mbrojtjeje psikologjike" përmes para-shpjegimit (prebunking), për të ndihmuar qytetarët të identifikojnë manipulimin para se ai të zërë rrënjë. Duke përfshirë të gjithë shoqërinë, shteti mund të mbrojë mjedisin informativ pa iu drejtuar censurës. Në fund, kjo qasje forcon sigurinë kombëtare duke ruajtur në të njëjtën kohë vlerat demokratike.

1. Prebunking - para-shpjegim

Ndërsa demaskimi (korrigjimi i një gënjeshtre pasi ajo është përhapur) është një mjet i domosdoshëm reaktiv, ai shpesh është më pak efektiv sepse gënjeshtra fillestare tashmë ka zënë rrënjë në mendjen e publikut. Para-shpjegimi (prebunking) i mëson qytetarët si të njohin *truket* e manipulimit, si emocionet e forta ose "ekspertët" e rremë, para se të hasin lajme të rreme. Duke informuar publikun për metodat e përdorura në NHMI, qeveria ndërton qëndrueshmëri afatgjatë të shoqërisë, duke e bërë dezinformimin më pak ndikues kur ai shfaqet. Kjo mund të arrihet në shumë mënyra.

- Mësim përmes lojës (gamified learning): Mjete interaktive, si loja "Bad News", u lejojnë përdoruesve të luajnë rolin e një aktori keqdashës. Duke përdorur teknika manipulimi për të fituar ndjekës të rremë, lojtarët mësojnë t'i dallojnë të njëjtat shenja paralajmëruese në burimet e tyre të informacionit.

- Video shpjeguese: video të shkurtra dhe neutrale që shpjegojnë truket e zakonshme të manipulimit, në vend që të trajtojnë histori specifike. Për shembull: një video mund të shpjegojë "scapegoating" (fajësimin e një pale), që kur ta shohësh në lajme, ta njohësh menjëherë si manipulim.

2. Parimi "Mos bëj dëm"

Çdo veprim i qeverisë duhet të balancohet me kujdes për të mbrojtur sigurinë kombëtare pa cenuar lirinë e shprehjes.

- Shmangia e rregullimit të tepruar: ligjet shumë të rrepta shpesh shkaktojnë një "efekt ftohës", ku platformat fshijnë më shumë përmbajtje sesa duhet për të shmangur gjobat e larta, gjë që kufizon debatin e shëndetshëm publik. Për ta parandaluar këtë, qeveritë duhet të shmangin ndalimin e përmbajtjes dhe në vend të kësaj të kërkojnë më shumë transparencë, si për shembull regjistra publikë të reklamave që tregojnë se kush ka paguar për reklama manipuluese. Kjo qasje i nxit platformat të përdorin etiketa dhe paralajmërime - të ngjashme me shiritat e verifikimit të fakteve të Meta-s - për të informuar përdoruesit për dezinformim të mundshëm pa i heshtur ata ose pa i fshirë postimet e tyre.

- Të synohet "Si-ja", jo "Çfarë": qeveria duhet të fokusohet në ndalimin e "mekanizmit" që qëndron pas gënjeshtrave. Kjo do të thotë të synohen "fermat e bot-eve" dhe llogaritë e rreme, në vend të mendimeve individuale, pasi është shumë më e sigurt për demokracinë të fshihen 10,000 profile të drejtuara nga kompjuterët sesa të censurohet një qytetar i vërtetë. Duke përdorur ligje si Ligji për shërbime digjitale (DSA), shteti mund t'u bëjë

presion kompanive të rrjeteve sociale që të forcojnë sigurinë e platformave të tyre, në mënyrë që ato të mos mund të shfrytëzohen më nga aktorë të huaj.

- Pavarësia: për të siguruar që përpjekjet kundër dezinformimit të mos keqpërdoren për përfitime politike, mbikëqyrja duhet të bëhet nga institucione të pavarura. Kjo përfshin rrjete për verifikimin e fakteve, media të besueshme, si dhe OJQ (si Alliance4Europe) që veprojnë si mbikëqyrës për të mbrojtur të drejtat digjitale. Duke fuqizuar ekspertë të pavarur në vend të politikanëve, shteti siguron që veprimet të synojnë vetëm kërcënimet reale të huaja. Kjo parandalon që mjetet kundër dezinformimit të keqpërdoren për përfitime politike.

3. Qasja gjithë-shoqërore

NHMI-ja është një kërcënim kompleks që nuk mund të zgjidhet nga një ministri e vetme; ajo kërkon një strategji kombëtare të koordinuar. Qeveria duhet të krijojë një trupë të unifikuar që përfshin Punët e Jashtme, Mbrojtjen, Punët e Brendshme dhe Arsimin, për të ndarë informacione dhe për të planifikuar përgjigjet. Duke komunikuar në mënyrë transparente me mediat e pavarura dhe OJQ-të, shteti forcon edukimin mediatik dhe ndërton një publik më të informuar pa ndërhyrje të drejtpërdrejtë të qeverisë.Ndërtimi i një shoqërie rezistente kërkon angazhim për arsimim në çdo nivel. Ministria e Arsimit duhet të integrojë edukimin mediatik në shkolla, duke u fokusuar në mënyrën se si funksionojnë sistemet demokratike dhe si përdoren narrativat për të manipuluar historinë ose shkencën. Ministria e Shoqërisë Informatike duhet të fokusohet në aftësitë digjitale, duke i ndihmuar qytetarët të kuptojnë si funksionojnë algoritmet e platformave dhe si të identifikojnë trendet "virale" të drejtuara nga bot-ët.

4. Bashkëpunimi ndërkombëtar

NHMI-ja është një kërcënim ndërkufitar që kërkon një rrjet për ta luftuar një rrjet tjetër. Duke u harmonizuar me kornizat evropiane, Maqedonia e Veriut mund të ketë qasje në mjete më të avancuara dhe të sigurojë që mjedisi i saj mediatik të përmbushë standardet demokratike ndërkombëtare.

- Paketa e Mjeteve NHMI: Qeveria duhet të miratojë Paketën e Mjeteve NHMI të BE-së, e cila përfshin monitorimin, zbulimin, sistemet e alarmit të shpejtë dhe përgjigjet diplomatike si sanksionet ndaj mediave të sponsorizuara nga shtetet e huaja.

- Forcimi i vetë-rregullimit: Inkurajimi i mediave për të ndjekur kodet e etikës profesionale dhe madje të aplikojnë për bashkëpunim dhe anëtarësim në Rrjetin Evropian të Standardeve të Kontrollit të Fakteve (EFCSN) ose Rrjetin global Ndërkombëtar të Kontrollit të Fakteve (IFCN).

Me miratimin e këtij modeli proaktiv dhe gjithëpërfshirës, Maqedonia e Veriut mund të mbrojë sigurinë e saj kombëtare duke forcuar - në vend që të dobësojë - të drejtat demokratike të qytetarëve të saj.

Институт за комуникациски студии



British Embassy Skopje

UK International Development
Partnership | Progress | Prosperity

Ky dokument është përgatitur në kuadër të programit „Forcimi i gatishmërisë operative për reagimin qeveritar ndaj FIMI-t në Maqedoninë e Veriut“, i financuar nga Qeveria e MB-së me mbështetjen e Ambasadës Britanike në Shkup. Përmbajtja e këtij publikimi nuk pasqyron domosdoshmërisht qëndrimin ose opinionet e Qeverisë së MB-së.