METODOLOGIA
de analiză a comportamentului în spațiul informațional

INTRODUCERE

Conform Strategiei securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr. 391/2023, una din **direcțiile de acțiune** în vederea realizării obiectivelor naționale de securitate și apărare, o reprezintă asigurarea rezilienței informaționale prin dezvoltarea cooperării dintre instituțiile publice, societatea civilă și mass-media în vederea contracarării influențelor informaționale amenințătoare (surse de informație sau tipuri de mesaje care pot crea panică, confuzie sau teamă în rândul populației. Aceste influențe pot proveni din diverse medii, precum mass-media, rețele sociale sau propagandă, și pot viza manipularea opiniei publice, răspândirea de dezinformare sau incitarea la violență. Ele pot afecta stabilitatea socială, încrederea în instituții și coeziunea socială).

Totodată, având în vedere statutul Republicii Moldova de stat candidat la aderarea la Uniunea Europeană, Centrul poate utiliza, ca repere metodologice orientative, instrumentele relevante dezvoltate la nivelul EEAS și al Uniunii Europene privind MIIS, riscurile sistemice și integritatea proceselor democratice, fără ca acestea să producă efecte juridice directe în ordinea națională.

I. DISPOZIȚII GENERALE

1. Prezenta metodologie (în continuare - Metodologie) reglementează activitatea la nivelul personalului responsabil de analiza comportamentului în spațiul informațional (analiza MIIS/DIMI) și interacțiunea acestuia cu alte subdiviziuni din cadrul Centrului pentru Comunicare Strategică și Contracarare a Dezinformării (CCSCD), precum și cu alte instituții de stat sau partenere. Ea stabilește cadrul conceptual și operațional pentru analiza fenomenului de manipulare informațională și ingerințe străine (în continuare - MIIS) și internă (domestic - DIMI).

2. Metodologia vizează înțelegerea modului în care actorii rău-intenționați - împreună cu activele lor digitale, entitățile implicate, fluxurile financiare și alte informații relevante - se infiltrează și se ascund în dezbaterea publică online, influențând opinii, decizii și percepții.

3. Aceasta oferă o abordare complementară centrată pe identificarea actorilor și a seturilor de manipulare informațională, ceea ce permite:

a) urmărire mai eficientă a modelului de comportament manipulator, orientarea capacităților analitice către amenințări relevante;

b) organizarea cunoștințelor privind ecosistemele de manipulare informațională;

c) anticiparea comportamentelor, rețelelor de colaborare și a campaniilor viitoare.

4. **Metodologia acoperă următoarele activități-cheie:**

a) **Identificarea actorilor primari**, în special sursa inițială de manipulare informațională la nivel de diseminare, inclusiv colectarea de informații din surse deschise, cu respectarea drepturilor și libertăților individuale așa cum sunt ele prevăzute în legislația națională și în normele internaționale ratificate de Republica Moldova, despre infrastructura digitală utilizată și despre entitățile afiliate;

b) **Identificarea și analiza MIIS/DIMI**, prin captarea, structurarea și interpretarea datelor relevante despre eforturile actorilor maligni;

c) **Monitorizarea continuă** a acestor fenomene și a evoluției lor în spațiul informațional;

d) **Raportarea și diseminarea produselor analitice**, într-o formă clară, operativă și orientată spre beneficiarii legali;

e) **Managementul cunoștințelor despre amenințări**, prin crearea și menținerea unei baze coerente și actualizate de date despre vectori de amenințare, narative manipulative și infrastructura informațională utilizată.

5. Elaborarea acestei metodologii răspunde nevoii de standardizare a proceselor de lucru și de uniformizare a produselor analitice emise de CCSCD. Această structurare unificatoare asigură:

a) mai bună asimilare a informației de către beneficiarii produselor;
b) procesare rapidă și relevantă a informațiilor captate;
c) menținerea relevanței analitice prin reacții prompte la evoluții în timp real;
d) consolidarea capacității instituționale de reacție și prevenție.

În cadrul prezentei Metodologii, sunt definite următoarele noțiuni:

Narativ de informație - definiția sublimată a unui enunț generic prin care se vizează livrarea unui anumit mesaj, idee sau comportament specific la nivelul consumatorului de informație. Spre deosebire de cele pozitive, narativele de informații maligne urmăresc influențarea non-transparentă a comportamentului publicului lor, determinarea unor convingeri care să influențeze o anumită decizie care este în interesul actorilor maligni și pe care aceștia din urmă nu o fac cunoscută.

Actor malign - acel individ sau entitate (statală sau non-statală) care promovează în mod conștient conținut manipulatoriu sau distorsionat menit a-l ajuta în atingerea unui scop politic, economic, social non-transparent și neasumat public care se află în contradicție cu interesele statului și ale cetățeanului, subminează instituțiile și procesele democratice în stat.

Canale maligne - acele canale de creare și de distribuire de conținut distorsionat, înșelător sau coordonat, în scop de influențare a opiniei publice înspre a accepta în mod inconștient sau neinformat o realitate deformată, care servește doar unui anumit grup/individ și ignoră interesul comun, de termen lung, al societății.

Canale pozitive - acele canale de creare și de distribuire a informațiilor care urmăresc buna și completa informare a cetățenilor, identificarea și corectarea unor informații false sau manipulatorii, conștientizarea la nivelul consumatorilor de informație a intențiilor manipulatorii manifestate de anumiți actori maligni, oferirea de clarificări referitoare la identitatea acestora, intențiile ascunse manifestate și legăturile cu actori maligni statali din exteriorul sau interiorul Republicii Moldova.

Canale neutre/necatalogate – acele canale de creare și de distribuire a informațiilor care prezintă nepărtinitor aspectele raportate sau despre a căror afinitate nu se pot face afirmații fără echivoc, fără să se implice în acțiuni de conștientizare

Termenul „tactici, tehnici și proceduri" (TTP) - descrie comportamentul unui actor malign (sau vector al unei amenințări informaționale) precum și cadrul structurat pentru punerea în aplicare a unei acțiuni de manipulare a informației și influență.

Manipularea informațională și ingerința străină (MIIS) - reprezintă model de comportament manipulator, desfășurat în mod intenționat și coordonat, care amenință sau are potențialul de avea un impact negativ asupra valorilor, a procedurilor și a proceselor politice, economice și sociale, promovat de actori statali sau nonstatali, inclusiv de intermediari din interiorul sau exteriorul statului, și care sunt de natură să cauzeze prejudicii securității, intereselor naționale sau obiectivelor naționale de securitate.

Deși se suprapune parțial cu dezinformarea, MIIS este definit de intenționalitatea coordonată a actorilor străini de a influența din exterior ecosistemul informațional și decizional al unui stat.

DIMI - Manipulare și interferență informațională internă (Domestic Information Manipulation and Interference - DIMI) reprezintă acțiuni deliberate întreprinse de actori rău-intenționați interni (persoane, grupuri sau entități naționale), care urmăresc distorsionarea sau manipularea informațiilor pentru a influența percepțiile, comportamentele și deciziile publicului din propriul stat DIMI implică utilizarea sistematică a narativelor manipulative, a dezinformării sau a conținutului distorsionat, diseminate prin canale media, rețele sociale sau alte mijloace de comunicare, în scopul realizării unor interese partizane, ideologice sau economice care contravin interesului public.

Acest fenomen reflectă adesea fragmentarea socială, polarizarea politică și instrumentalizarea spațiului informațional de către actori autohtoni. Deși poate fi exploatat sau amplificat ulterior de actori străini, DIMI se distinge prin inițiativa și coordonarea exclusiv internă a manipulării, fără a presupune prezența sau controlul unui actor străin în faza sa inițială.

Metodologie - ansamblul metodelor, tehnicilor, procedeelor și acțiunilor utilizate la analiza informațiilor și evaluarea riscurilor, având în vedere clarificarea înțelesului conceptelor prin definirea corectă a acestora.

Instrumentele analitice - sunt metode, tehnici, software sau dispozitive utilizate pentru a colecta, procesa, analiza și interpreta date, în scopul de a extrage informații relevante și de a sprijini luarea deciziilor.

Proces de analiză - ansamblul activităților specifice, realizate în mod sistematic de către analist, pentru obținerea produsului analitic.

Produs analitic - produs finit al procesului de analiză, materializat sub forma raportului de analiză.

Produs de suport analitic - materiale grafice de diferite categorii, care susțin și însoțesc produsul analitic, dar nu reprezintă rezultatul demersurilor analitice.

Campaniile de comunicare strategică - reprezintă un ansamblu de acțiuni planificate și coordonate, concepute pentru a transmite mesaje specifice unui public țintă, cu scopul de a influența percepțiile, comportamentele sau atitudinile acestuia în direcția obiectivelor stabilite. Aceste campanii sunt utilizate în diverse contexte, precum afaceri, politică, securitate, sănătate publică sau educație, pentru a sprijini misiuni strategice sau obiective pe termen lung.

Dezinformarea - informație al cărei caracter fals sau înșelător poate fi verificat, care este creată, prezentată și răspândită pentru a obține un câștig economic sau pentru a induce, în mod deliberat, publicul în eroare și care poate provoca un prejudiciu public. Prejudiciul public cuprinde amenințările la adresa proceselor politice, principiilor și valorilor democratice și a proceselor de elaborare a politicilor, precum și amenințările

la adresa bunurilor publice, a protecției sănătății cetățenilor, a mediului sau a securității;

Propaganda - acțiune de răspândire sistematică a informației pentru influențarea atitudinilor, convingerilor și comportamentului persoanelor, pentru susținerea sau compromiterea anumitor instituții, cauze ori persoane prin prezentarea manipulatorie a informației și/sau prin reflectarea selectivă a evenimentelor, în scopul subminării intereselor naționale ale statului. Spre deosebire de dezinformare, propaganda nu implică neapărat informații false, ci poate folosi și informații adevărate prezentate într-un mod distorsionat sau părtinitor.

Manipularea - este influențarea intenționată a gândurilor, emoțiilor sau comportamentelor unei persoane sau ale unui grup, de obicei într-un mod subtil sau înșelător, cu scopul de a obține un avantaj sau de a controla deciziile acestora. Manipularea poate să apară în relații interpersonale, în comunicarea de masă, în politică, afaceri sau alte contexte sociale.

Informații - set de date prelucrate și plasate în contexte de interes. Informațiile sunt prezentate, de regulă, sub formă de „publicații" și au nivel de agregare redus. Atât datele, cât și informațiile, nu au la bază demersuri analitice.

Date - descrieri simple de aspecte, situații, elemente, stări de fapt etc. (exemplu: data și numărul publicațiilor, interacțiunile, modus operandi, coordonatele geografice, produsul intern brut pe ultimii zece ani, rata de schimb valutar etc.). Dat fiind faptul că prezintă cel mai ridicat nivel de agregare, datele sunt deseori folosite pentru elaborarea de statistică.

Predicție - aserțiune sub forma rezultatului operației raționale de anticipare a evenimentelor.

Tendință (trend) infracțională - direcție evolutivă, identificată pe baza repetabilității faptelor/analizei, pe care o înregistrează un fenomen.

Tipar (pattern) infracțional - model generic privind structura activităților, proceselor, ori fenomenelor acțiunilor, caracterizat prin elemente specifice (modus operandi, locul și timpul acțiunii, public target etc.), însă despre care nu sunt suficiente date/informații care să confirme legătura de cauzalitate între acestea.

Beneficiar al analizei - solicitant, client al analizei și toți cei care folosesc rezultatele acesteia, priviți integrat.

Bază de date - modalitate de stocare a datelor/informațiilor pe suporturi electronice, cu posibilitatea accesării acestora.

Categorisire - repartizare, triere, catalogare a datelor/informațiilor, în funcție de criteriile stabilite, pe tipuri, clase, niveluri etc.

Categorie **-** reprezintă un grup sau o clasă de elemente care împărtășesc caracteristici, proprietăți sau trăsături comune. Este un mod de organizare sau clasificare care permite gruparea obiectelor, ideilor sau fenomenelor pe baza unor criterii definite.

Strategie - viziune de perspectivă, de regulă pe termen mediu și lung, asupra modului în care este preconizată desfășurarea activității specifice.

Capacitate – potențial (uman/ financiar/ material/ tehnic/ informațional/ administrativ/ normativ etc.) al entităților de a-și îndeplini competențele/ misiunile/ atribuțiile, exprimat ca raport între necesar și starea de fapt.

Analiza calitativă - este un proces de examinare și interpretare a datelor non-numerice (cum ar fi texte, interviuri, imagini sau observații) pentru a înțelege concepte,

opinii, experiențe sau fenomene sociale. Acest tip de analiză se concentrează pe interpretarea semnificațiilor și pe identificarea tiparelor sau relațiilor care nu pot fi cuantificate în mod direct.

Analiza cantitativă - este un proces de examinare a datelor numerice sau măsurabile pentru a testa ipoteze, a identifica tipare și a trage concluzii statistice. Aceasta implică colectarea, procesarea și interpretarea informațiilor cuantificabile, fiind utilizată pentru a generaliza rezultatele la o populație mai mare.

Risc - reprezintă probabilitatea ca un eveniment sau o situație să aibă un impact negativ asupra securității, stabilității sau dezvoltării unei țări și a societății sale. Acesta poate apărea din factori interni sau externi și afectează populația, instituțiile, economia și resursele naționale.

Foresight - reprezintă procesul sistematic și anticipativ de explorare a viitorului, utilizat pentru a identifica tendințe, incertitudini și posibile scenarii care pot influența evoluția unui domeniu, a unei organizații sau a unei societăți. Scopul foresight-ului este de a sprijini luarea deciziilor strategice prin pregătirea pentru oportunități și riscuri viitoare.

Interacțiunile - pe platformele de social media reprezintă suma aprecierilor, comentariilor și distribuirilor asociate unui conținut, reflectând nivelul de implicare al utilizatorilor față de acesta.

II. Identificarea MIIS/DIMI

6. Scopul identificării

6.1. Etapa de identificare are ca scop detectarea inițială a unor posibile campanii de manipulare și ingerință informațională (MIIS/DIMI), înainte de demararea procesului complet de analiză. Ea presupune validarea existenței unui SMI (Set de Manipulare Informațională) și încadrarea acestuia într-un cadru de prioritizare strategică.

6.2. Un SMI este considerat valid atunci când există indicii convergente privind coordonarea între mai multe active digitale (ex. reutilizare de conținut, sincronizare temporală, elemente tehnice comune).

6.3. Delimitarea între SMI-uri diferite se realizează pe baza diferențelor de infrastructură, narative sau obiective operaționale, chiar și în cazul în care acestea aparțin aceluiași actor.

7. Puncte de pornire în procesul de identificare

Analizele pot începe, în general, din două direcții principale:

a) **Identificarea unei prezențe suspecte a unei narațiuni** în spațiul online (ex. social media, platforme alternative, forumuri, evenimente offline etc.), urmată de analiza distribuției inițiale pentru a verifica dacă entitățile implicate fac parte dintr-un SMI (ex. Storm 1516, Matryoshka, Doppelgänger și altele);

b) **Recepționarea unui semnal extern** sub forma unui raport public sau privat (din partea mass-mediei, cercetătorilor, ONG-urilor, partenerilor comerciali, agențiilor de stat etc.) care indică existența unui comportament inautentic coordonat (CIC), a unei operațiuni de influență sau a unui SMI. Aceste rapoarte trebuie tratate ca puncte de plecare, constatările trebuie verificate, completate și confirmate cu datele proprii, întrucât pot conține omisiuni sau bias intenționat/neintenționat.

8. Surse de informație pentru identificare

Printre sursele utile în această etapă se numără:

a) monitorizarea activă a rețelelor sociale și a spațiului web;

b) alertele provenite de la platforme partenere sau servicii OSINT automatizate;

c) raportările de la companii tehnologice, centre de cercetare, mass-media, think-tankuri etc.;

d) analize independente sau colaborative;

e) surse deschise.

9. **Prioritizarea SMI-urilor pentru analiză**

Resursele fiind limitate, este esențial ca analiza detaliată să vizeze în mod prioritar SMI-urile care amenință **interesele naționale fundamentale** (ex. suveranitatea, securitatea, coeziunea socială etc.);

10. Analiza trebuie să includă **identificarea publicurilor țintă sau afectate**, precum și modul în care mesajele sunt adaptate pentru acestea. Înțelegerea diferențelor între segmente (ex. urban/rural, vorbitori de limbi diferite, diaspora etc.) este esențială pentru evaluarea impactului și pentru formularea răspunsului.

11. **Recomandări generale**

a) Triangularea informațiilor este esențială înainte de trecerea la analiza aprofundată;

b) Este important să se documenteze indicatorii tehnici inițiali chiar dacă aceștia par neconcludenți în faza incipientă;

c) Fiecare caz nou trebuie analizat și raportat sistematic, astfel încât să contribuie la construirea unei arhive de referință pentru SMI-uri recurente sau ce suferă mutații.

III. Analiza MIIS/DIMI

12. **Scopul analizei:**

Analiza are ca obiectiv principal identificarea, cartografierea și înțelegerea comportamentului și a infrastructurii utilizate de actorii rău-intenționați în desfășurarea campaniilor de manipulare informațională și ingerință, fie ele de natură străină (MIIS) sau internă (DIMI). Analiza vizează atât activele digitale implicate, cât și rețelele de conexiuni, tacticile de operare și, acolo unde este posibil, identificarea actorilor din spatele acestora.

Analiza nu reprezintă un scop în sine, ci un instrument de sprijin pentru formularea răspunsului instituțional. Rezultatele analizei trebuie să permită derivarea unor opțiuni de acțiune în domeniul comunicării strategice, al politicilor publice sau al intervenției operaționale, în funcție de natura și gravitatea fenomenului identificat.

13. **Punctul de pornire în analiză**

Procesul analitic începe de regulă de la unul sau mai multe elemente tehnice detectabile, precum:

13.1. conturi de social media; site-uri web; canale de comunicare; adrese IP; identități vizuale; indicii lingvistice sau stilistice; orice alt element digital reutilizat sau recognoscibil care permite extinderea analizei.

Acestea sunt utilizate pentru a extinde analiza și a construi harta completă a infrastructurii informaționale implicate.

14. **Conceptul de SMI**

În cazul MIIS sau DIMI, ansamblul de active digitale interconectate este denumit Set de Manipulare Informațională.

Obiectivul echipei este consolidarea cunoștințelor despre acest SMI prin:

a) conectarea tehnică și contextuală a tuturor elementelor componente;
b) înțelegerea relațiilor dintre entitățile implicate;
c) documentarea scopului, structurii și funcționării rețelei.

15. **Exemple de activități analitice**

Analistul poate desfășura o serie de activități analitice, precum:

a) identificarea altor site-uri afiliate SMI;
b) detectarea conturilor de social media care reutilizează aceleași elemente vizuale, descrieri, conținuturi sau linkuri;
c) analizarea instrumentelor și tehnologiilor utilizate pentru automatizare, anonimizare, disimulare sau manipulare;
d) corelarea comportamentelor de postare;
e) utilizarea instrumentelor OSINT pentru extragerea de date din surse deschise;
f) și alte activități preluate din bunele practici în domeniul de referință al metodologiei.

16. **Identificarea operatorilor** Atunci când este posibil, se recomandă identificarea entităților care coordonează SMI-ul. Acest pas este esențial pentru:

a) atribuirea clară a campaniei către un actor rău-intenționat;
b) stabilirea caracterului străin (MIIS) sau intern (DIMI) al sursei;
c) înțelegerea scopurilor, strategiilor și mecanismelor de amplificare.

IV. Monitorizarea SMI-urilor

17. **Obiectivul monitorizării**

Odată ce un SMI este identificat, procesul de lucru nu se încheie cu analiza sa.

Urmează o etapă critică: monitorizarea continuă. Aceasta vizează urmărirea activității în timp, pentru a detecta reactivări, adaptări tactice sau extensii ale rețelei, indiferent dacă SMI-ul a fost atribuit sau nu unui actor concret.

De asemenea, chiar și în absența unui SMI conturat complet, orice rețea sau activitate suspectă care indică semne de coordonare, recurență sau potențial de influență malignă, trebuie supusă monitorizării. Lipsa atribuirii sau a unui model complet nu justifică suspendarea supravegherii, ci dimpotrivă, argumentează necesitatea unei urmăriri proactive.

18. **Exemplu practic**

Dacă un SMI a fost identificat ca folosind IP-ul 176.123.0.83, se poate configura o alertă DNS care notifică analistul ori de câte ori un domeniu nou este înregistrat pe acel IP. Astfel, reactivarea rețelei poate fi detectată chiar înainte ca narațiunile să fie publicate, oferind timp pentru răspuns proactiv.

*IP-ul a fost scris aleatoriu orice corespundere cu unul real este o coincidență.

V. Managementul Cunoștințelor despre Amenințări și Reutilizarea Analizei

19. **Scopul gestionării cunoștințelor** În procesul de contracarare a manipulării informaționale, acumularea de date și învățăminte are valoare doar în măsura în care este stocată, organizată și reutilizabilă. Gestionarea eficientă a cunoștințelor permite:

a) păstrarea memoriei instituționale;
b) evitarea duplicării eforturilor;
c) fundamentarea rapidă a deciziilor;
d) accelerarea reacțiilor în situații operative.

20. **Componentele unui sistem eficient de management al cunoștințelor**

Un sistem eficient trebuie să includă, în mod integrat, următoarele componente:

20.1. Depozit documentar (rapoarte, note, alerte, fișe informative)

Toate rapoartele - interne sau externe - privind SMI-uri identificate sau monitorizate trebuie arhivate într-un depozit de documente căutabil, care permite:

a) trasabilitatea (autor, dată, sursă, etichete etc.);
b) căutarea în text complet;
c) filtrarea prin operatori logici (AND, OR, NOT) și intervale de timp.

21. **Beneficii strategice**

Un sistem eficient de management al cunoștințelor permite:

a) construirea de profiluri dinamice ale actorilor rău-intenționați;
b) reutilizarea logică a produselor analitice, în locul reluării procesului de la zero;
c) schimbul standardizat de date cu parteneri naționali și internaționali;
d) automatizarea proceselor de alertare, identificare și raportare;
e) asigurarea continuității instituționale, chiar în condiții de rotație a personalului sau presiune de timp.

VI. Raportare și Diseminare

22. **Scopul raportării**

Procesul de analiză și monitorizare are valoare operațională numai în măsura în care constatările sunt **transmise în timp util** către actorii relevanți, interni și externi, care pot lua măsuri concrete.

23. **Destinatarii produselor analitice**

Raportarea nu se limitează la structurile interne CCSCD. În funcție de natura și impactul constatărilor, **produsele analitice pot fi diseminate, integral sau parțial, către:**

a) instituții guvernamentale sau de reglementare;
b) autorități cu rol în securitatea cibernetică, protecția datelor sau ordinea constituțională;
c) parteneri internaționali;
d) alte structuri publice care gestionează comunicarea strategică sau relația cu mass-media.

24. **Rigoare, trasabilitate și siguranță**

Toate produsele trebuie redactate conform unor **standarde de trasabilitate, validare și clasificare**, pentru a evita riscurile de dezinformare accidentală sau de scurgere de informații sensibile.

Este recomandată utilizarea unui format standardizat (fișe analitice, note de alertă, rapoarte de evaluare etc.), cu marcaj de confidențialitate și sistem de distribuire controlată.

25. Utilizarea analizei în răspunsul strategic

Produsele analitice trebuie să permită nu doar înțelegerea fenomenului, ci și formularea unor direcții de acțiune. În funcție de caz, acestea pot include:

- recomandări de comunicare strategică (clarificări publice, reformularea mesajelor instituționale, implicarea unor mesageri credibili);
- informarea și alinierea actorilor instituționali și non-instituționali relevanți;
- sprijinirea procesului decizional la nivel guvernamental sau interinstituțional.

Analiza devine astfel un element integrat în ciclul de răspuns, contribuind la prevenirea, limitarea sau contracararea efectelor MIIS/DIMI.

25. Concluzie

Raportarea nu este un act birocratic, ci o acțiune strategică.

Produsele analitice trebuie concepute pentru a genera reacții, decizii și intervenții concrete. Diseminarea inteligentă și direcționată a informației este o condiție fundamentală pentru ca analiza să contribuie efectiv la apărarea spațiului informațional al Republicii Moldova.