CENTRUL PENTRU
COMUNICARE STRATEGICĂ
ȘI COMBATERE A DEZINFORMĂRII

# TACTICI MALIGNE ÎN SPAȚIUL INFORMAȚIONAL

## Ghid de buzunar al utilizatorului conștient

CHIȘINĂU
2025

# 1.COMPORTAMENT INAUTENTIC COORDONAT

Rețea de conturi care par diferite, dar sunt controlate din aceeași sursă. Postează aceleași sensuri, conținut, mesaje în același timp pentru a crea iluzia unei majorități și interes sporit.

## Care e pericolul?

Schimbă artificial discuțiile publice și creează presiune socială, ca și cum ar exista o majoritate spontană.

- În februarie 2019 Meta a șters peste 160 de conturi și 28 de pagini care făceau campanie politică ascunsă în spațiul informațional din Moldova. În octombrie 2024, o altă rețea cu 7 conturi, 23 de pagini, un grup și 20 de conturi de Instagram a fost blocată pentru conținut fals.
- În România, la începutul lui 2025, Meta a închis 658 de conturi și 14 pagini care se dădeau drept localnici și au cheltuit peste 170.000 USD pe reclame politice ascunse.

## Cum te aperi?

- Observă dacă mesajele identice apar la aceeași oră, pe conturi necunoscute.
- Verifică cine administrează pagina și cine plătește reclamele.
- Nu distribui pe impuls. Raportează conturile suspecte.

# 2.REȚEA DE CONTURI INAUTENTICE

Rețelele de conturi inautentice sunt seturi de profile false sau controlate centralizat, care publică și amplifică același conținut pentru a crea impresia de popularitate.

## Care e pericolul?

Crează tendințe și manipulează algoritmii rețelelor sociale pentru a promova artificial conținut politic sau conspirații spre public. Manipulează percepția publică privind importanța subiectului.

- În România, doar în 2024–2025, platformele au eliminat peste 59.000 de conturi false, au blocat 1,3 milioane de urmăritori falși și 1,5 milioane de like-uri artificiale.

## Cum te aperi?

- Verifică vechimea contului și istoricul postărilor.
- Caută sursa inițială.
- Compară afirmațiile cu surse de încredere.
- Raportează conturile suspecte ca „înșelătorie/spam”.

# 3.IMPERSONAREA INSTITUȚIILOR SAU PERSOANELOR REALE

Conturi sau pagini care se prezintă ca instituții ori persoane cunoscute, fără să aibă legătură reală cu ele. Unele se ascund sub eticheta de „parodie”, dar urmăresc să dezinformeze și să manipuleze.

## Care e pericolul?

Distribuirea informațiilor false, colectarea datelor și slăbirea încrederii în paginile reale ale instituțiilor.

**Cum le recunoști?**

- Denumire aproape identică cu pagina oficială.
- Fotografii clonate.
- Lipsa bifei de autenticitate.
- Creare recentă fără activitate regulată.

## Cum te aperi?

- Verifică dacă există ecuson verificat.
- Vezi dacă există conexiuni cu alte pagini oficiale.
- Raportează contul ca „falsificare identitate”.

# 4.CONȚINUT FABRICAT CU INTELIGENȚĂ ARTIFICIALĂ

Conținut fabricat digital cu ajutorul inteligenței artificiale: texte, imagini sau filmări create pentru a imita declarații și evenimente reale, cu scopul de a manipula percepția publică.

## Care e pericolul?

Producția falsurilor credibile și răspândirea neîncrederii în instituțiile statului, presă și surse de încredere.

**Cum le recunoști?**

- Mișcarea nenaturală a buzelor și vocii, privire fixă.
- Lumini sau umbre denaturate.
- Conturi noi create.

## Cum te aperi?

- Verifică dacă materialul apare și în alte surse de încredere.
- Caută greșeli vizuale și mențiunea „creat digital”.
- Nu distribui până nu ești sigur că e un produs autentic.

# 5.DOCUMENTE TRUCATE ȘI FABRICATE

„Ordine”, „note”, „circulare” sau „comunicate” care imită formatul instituțional. Nu sunt emise de instituții, dar circulă și sunt prezentate ca oficiale.

## Care e pericolul?

Distribuirea informațiilor false, colectarea datelor și slăbirea încrederii în paginile reale ale instituțiilor.

**Cum le recunoști?**

- Denumire aproape identică cu cea a entității oficiale.
- Date de contact greșite.
- Greșeli de scriere, datare eronată, logo-uri vechi, formulare incoerentă, nume ale persoanelor care nu mai sunt în funcție.

## Cum te aperi?

- Verifică pe site-ul oficial sau la instituția emitentă daca există acest document.
- Verifică sursa/canalul prin care ai primit documentul.