Exercițiu introductiv de securitate cibernetică și război informațional

Nivel: Anul II, studii de Securitate

Durată: 120 minute

CyberTransilvanica este un exercițiu narativ de simulare a unui incident cibernetic minor transformat într-o criză informațională majoră. Studenții sunt puși în roluri instituționale, mediatice și civice, pentru a înțelege cum o pană de curent locală devine o armă informațională în contextul statului fictiv Carpathia.

Exercițiul urmărește dinamica dintre securitatea cibernetică și încrederea publică, accentuând dimensiunea strategică a comunicării și importanța gândirii critice.

Scopul este de a dezvolta capacitatea de analiză strategică, gândirea critică și înțelegerea interacțiunii dintre spațiul cibernetic și cel societal. Într-o societate interconectată, securitatea cibernetică nu înseamnă doar protejarea sistemelor, ci și protejarea minților.

Exercițiul are un nivel tehnic elementar, iar accentul cade pe **gândire critică, comunicare, evaluarea surselor și reacția instituțională sub presiune**.

Context narativ – Pană de curent și furtuna informațională în Carpathia

La primele ore ale dimineții în Carpathia, mai multe spitale din două județe rămân fără energie electrică— în scurt timp alimentarea cu energie electrică este trecută pe generatoare. Compania regională de distribuție a energiei electrice (CER) transmite la 08:10 un comunicat scurt: „Pană de curent cauzată de un incident tehnic. Echipele noastre acționează pentru remediere."

În locul calmului, însă, se instalează o furtună informațională. La 08:20, pe rețele sociale și în grupuri de mesagerie apar postări care susțin că a fost un atac cibernetic coordonat împotriva un instituții ale Carpathiei: clipuri parțial editate, capturi de e-mail scoase din context, conturi nou-create care răspândesc acuzații privind incompetența autorităților naționale și locale.

În mai puțin de o oră, un incident tehnic se transformă în criză de încredere publică: hashtaguri precum #BlackoutCarpathia și #GuvernulAscunde devin virale, iar mass-media preia narațiuni contradictorii fără verificări riguroase.

*Pe fondul emoției colective, actorii instituționali sunt nevoiți s**ă restabilească funcționarea unor infrastructuri critice rapid** și să comunice **adevărul într-un haos informational.***

Obiective

- Înțelegerea modului în care **dezinformarea poate amplifica un incident cibernetic minor**.
- Identificarea **actorilor, narațiunilor și tacticilor** specifice războiului informațional.
- Exersarea reacțiilor instituționale și jurnalistice într-un **context de presiune informațională**.
- Dezvoltarea competenței de **evaluare a surselor** și a **gândirii critice**.
- Înțelegerea legăturii dintre **comunicarea strategică, securitatea cibernetică și reziliența societală**.

Actorii implicați (echipele de joc)

Echipa	Rol principal	Obiectiv
Ministerul Digitalizării/ CERT Carpathia	Gestionarea crizei și comunicarea publică	Restabilirea încrederii și prevenirea panicii
Compania Energetică Regională (CER)	Clarificarea cauzei tehnice	Transparență și acuratețe în informare
Mass-media & fact checkeri	Gestionarea fluxului de informații	Verificarea surselor și evitarea senzaționalismului
Publicul / Rețelele sociale/ Influenceri	Opinie publică, reacții online	Testarea impactului emoțional al informațiilor
Actorul străin (Umbrosia)	Inițierea și amplificarea dezinformării	Subminarea încrederii în autorități

Etapă/	Durată/	Activitate
Briefing	*15 min*	Prezentarea contextului narativ și a regulilor jocului.
Simulare (faza activă)	*90 min*	Fiecare echipă reacționează la injecturile lansate din 15 în 15 minute.
Debriefing	*30–45 min*	Analiză, reflecție asupra securității cibernetice și discuție despre comunicare, percepție, vectorii de atac și manipulare.

Reguli generale de participare

- Fiecare echipă trebuie să **rămână în rol** și să acționeze realist, conform responsabilităților atribuite.
- Comunicarea se face prin **mesaje scurte, clare și argumentate**, nu prin afirmații emoționale.
- Toate deciziile și reacțiile trebuie să fie **scrise** (comunicate, postări, articole, declarații etc.).
- Informațiile primite de la moderator/ profesor trebuie tratate **ca evenimente reale**.
- Obiectivul nu este „câștigul”, ci **analiza mecanismelor informaționale și a impactului decizional**.

Ce trebuie să faceți?

- ✓ Citiți cu atenție fișa echipei voastre (rol, obiectiv, restricții).
- ✓ Reacționați la fiecare „inject” (știre, postare, comunicat care se adaugă narațiunii inițiale) în timp real.
- ✓ Luați decizii, comunicați și documentați fiecare reacție.
- ✓ Pregătiți-vă pentru o discuție finală despre modul în care informația a modelat securitatea cibernetică, percepția asupra acesteia și comportamentul public.

1. Ministerul Digitalizării în subordinea căruia este CERT Carpathia

Rol: analiza și investigarea incidentului, comunicarea oficială, menținerea încrederii.
Obiectiv: remedierea incidentelor cibernetice și asigurarea continuității, calmarea populației, contracararea panicii, coerență instituțională.

După fiecare inject:

Analizează impactul politic și public al evenimentului.

Decide **dacă reacționează imediat** sau așteaptă verificări suplimentare.

Redactează un **comunicat scurt (3–5 fraze)** sau o **declarație oficială**.

Poate solicita sprijinul Companiei Energetice (CER) pentru date tehnice.

Dacă este cazul, convoacă o „conferință de presă simulată” (prin citirea mesajului public).

Produse generate:

Comunicat oficial, declarație publică, briefing de presă.

> ***Exemplu:***
>
> *„Ministerul Digitalizării confirmă că incidentul este de natură tehnică și nu există dovezi privind un atac cibernetic. Echipele tehnice ale CER lucrează pentru restabilirea completă a rețelei.”*

2. Compania Energetică Regională (CER)

Rol: sursă tehnică de informație și clarificare.

Obiectiv: menținerea transparenței, transmiterea datelor reale, combaterea zvonurilor.

După fiecare inject:

Verifică veridicitatea informațiilor care implică sistemul energetic.

Emite un **update tehnic clar**, fără termeni emoționali.

Coordonează mesajele cu Guvernul (evită contradicțiile).

Poate solicita corectarea publică a știrilor false (prin media).

Produse generate:

Comunicat tehnic, infografic explicativ, update de progres.

Exemplu:

„Sistemele de control funcționează normal. Alimentarea a fost reluată în proporție de 95%. Nu există urme ale unui acces extern."

3. Mass-media & fact-checkeri

Rol: intermedierea informației între instituții și public.
Obiectiv: verificarea surselor, evitarea senzaționalismului, combaterea dezinformării.

După fiecare inject:

Verifică autenticitatea informației (sursa, autorul, timestamp-ul, conținutul).

Decide **dacă publică sau nu** informația.

Redactează un **titlu de articol** sau un **mesaj fact-check**.

Poate cere reacții oficiale de la Ministerul Digitalizării sau CER.

În fazele tensionate, organizează o „dezbatere media" scurtă între jurnaliști pentru analiza situației și a reacției.

Produse generate:

Articol de presă (150–200 cuvinte), titlu, reacție de tip fact-check.

Exemplu:

„#FactCheck: Nu există confirmări oficiale privind un atac cibernetic. Compania Energetică Regională a transmis că incidentul are cauze tehnice.”

4. Publicul / Rețele sociale / Influenceri

Rol: oglinda emoțională a societății.
Obiectiv: testarea impactului și răspândirii informației.

După fiecare inject:

Postează 2–3 mesaje scurte (max. 280 caractere) care reflectă reacții tipice: panică, ironie, indignare, sprijin etc.

Decide dacă redistribuie sau contestă o informație.

Poate crea un sondaj informal („Crezi că Guvernul spune adevărul?”).

Poate reacționa la comunicatele oficiale.

Produse generate:

Postări (texte, meme, comentarii), reacții la mesaje publice.

Exemplu:

„Guvernul zice că nu e atac… dar atunci de ce s-a stins tot orașul? 🤔 #BlackoutCarpathia”

5. Actorul străin (statul adversar Umbrosia)

Rol: destabilizare strategică, amplificare a haosului informațional.
Obiectiv: erodarea încrederii în autorități, polarizarea populației.

După fiecare inject:

Lansează 1–2 narațiuni alternative sau conspiraționiste.

Folosește tehnici de manipulare: *apel la emoții, framing, falsuri*

Exploatează greșelile de comunicare ale celorlalți.

Amplifică prin hashtaguri, „surse anonime” și insinuări.

Produse generate:

Postări manipulative, „documente” falsificate, citate scoase din context.

Exemplu:

„Nu e prima dată când Carpathia e ținta unui atac cibernetic. De ce tace Guvernul? De ce se ascund cauzele incidentului? #GuvernIncompetent #GuvernulTace #Incompetenți

Cum se evaluează reacțiile echipelor?

Criteriu	**Indicator**	**Scor (0–5)**
Claritate	Mesaje concise, coerente, fără ambiguitate	☐
Acuratețe	Reacții bazate pe date, nu pe presupuneri	☐
Coordonare	Consistență între echipe (Guvern–CER–Mass-media)	☐
Impact	Eficiența în limitarea dezinformării / panicii	☐
Inovație	Soluții creative și realiste de contracarare	☐

Tabel-sinteză rapidă

Echipă	**Tip de reacție după fiecare inject**	**Timp de răspuns**	**Forma livrabilului**
Ministerul Digitalizării/ CERT	Investigații/ Comunicat oficial / Declarație publică	10 min	Text scris, 5 fraze max.
CER	Comunicat tehnic / Update de progres	10 min	Text scurt, date concrete
Mass-media	Articol / Fact-check / Titlu de știre	10 min	3 paragrafe
Public / Rețele	Postări, comentarii, reacții online	8–10 min	2–3 postări (max. 280 caractere)

Echipă	Tip de reacție după fiecare inject	Timp de răspuns	Forma livrabilului
Umbrosia	Mesaje false, narațiuni alternative	8–10 min	Text / imagine / video fals (utilizati AI)

INJECT 1 — T+15 min

Titlu: Comunicat oficial inițial (actualizat)

Descriere: CER publică un comunicat: „Pană de curent cauzată de un incident tehnic. Alimentarea s-a mutat pe generatoare; echipele acționează.” Comunicatul include un paragraf tehnic sumar (fără detalii sensibile).
Actori vizați: Ministerul Digitalizării / CERT, CER, Mass-media
Efect urmărit: Ancorarea cadrului factual — verificăm dacă instituțiile răspund coordonat.
Sarcini (ce trebuie să producă fiecare echipă):

Ministerul Digitalizării / CERT: trimite notă internă (privată) către echipele de răspuns la incident de securitate cibernetică: solicitare colectare loguri privind sistemele informatice ale CER/ loguri privind sistemele critice; pregătește comunicat scurt de susținere publică în 10 min.

CER: publică comunicatul (text de 3–5 fraze). Inițiază colectarea logurilor relevante asupra sistemele informatice.

Mass-media / Fact-check: publică știrea pe baza comunicatului; cere clarificări tehnice.

Public / Influenceri: postează observații locale (2–3 postări).

Umbrosia: monitorizează și pregătește prima serie de micro-postări care pun sub semnul întrebării lipsa detaliilor tehnice.

Notițe: Se publică comunicatului CER către toate echipele; se evaluează calitatea reacției și timpul de reacție al fiecărei echipe.

Livrabile așteptate: Comunicat CER publicat; notă internă CERT; 1–2 articole media inițiale.

INJECT 2 — T+30 min

Titlu: Hashtag viral & conturi nou-create
Descriere: Apare hashtagul **#BlackoutCarpathia**; mai multe conturi nou-create susțin că a fost „atac cibernetic coordonat”. Volumele pe social cresc rapid.
Actori vizați: Public/Influenceri, Mass-media, Umbrosia
Efect urmărit: Testarea capacității instituțiilor de monitorizare (signal detection) și a reacției media la presiunea socială.
Sarcini:

Ministerul Digitalizării / CERT: activează monitorizarea OSINT (volume, top conturi) și identifică 3 conturi cu activitate suspicioasă; decide dacă emite mesaj de calmare sau așteaptă investigații.

CER: publică un update tehnic scurt (procente alimentare / spitale prioritare) pentru a oferi date verificabile.

Mass-media / Fact-check: publică un fact-check inițial: cine a creat conturile? (dacă nu există confirmare, marcăm ca „neconfirmat”).

Public / Influenceri: generează 3 tipuri de postări (ex. panică, solicitare de informații, sfaturi practice).

Umbrosia: lansează micro-postări pentru a amplifica îndoiala („De ce nu se publică informațiile tehnice detaliate? Cine blochează accesul la informații și de ce?”).

Outputuri așteptate: Raport OSINT scurt (CERT), update CER, fact-check media, set de postări publice reprezentative.

INJECT 3 — T+45 min

Titlu: Captură-e-mail aparență internă (falsificare)

Descriere: Pe rețeaua de socializare ClokClok apare o captură aparent internă ce conține textul „Nu publicați nimic până nu primim instrucțiuni centrale.” Documentul pretins arată ca un e-mail între birouri locale și conducerea CER.
Actori vizați: Ministerul Digitalizării / CERT, Mass-media, Umbrosia
Efect urmărit: Forțarea verificării autenticității; testarea procedurilor de răspuns la scurgeri (leaks).

Sarcini:

Ministerul Digitalizării / CERT: pornește verificarea pentru verifica autenticitatea. Emite poziție preliminară: „se investighează autenticitatea.”

CER: verifică dacă expeditorul/contul există în sistemele interne; pregătește un scurt raport despre procedurile interne de comunicare pe care îl publică.

Mass-media / Fact-check: analizează datele preliminare, contactează surse diverse și verifică autenticitatea, publică video pe ClokClok.

Public / Influenceri: distribuie conținutul mass-media / contestă documentul; se cer demisii, se generează clipuri virale pe ClokClok.

Umbrosia: adaugă comentarii insinuante la postările de pe ClokClok („așa se mușamalizează, „incompetenții ascunde informații vitale”, „incompetența celor care ne conduc ucide. securitatea cibernetică a spitalelor e varză”).
Notițe moderator: Se evaluează modalitatea în care echipele decid dacă documentul e fals sau rael.

Livrabile așteptate: Poziție preliminară CERT; postare fact-check; reacții și comentarii publice polarizante, comentarii insinuante pe ClokClok

INJECT 4 — T+60 min

Titlu: Clip scurt manipulat (fragment audio/video)
Descriere: Pe ClokClok apare un clip scurt, editat, în care un oficial CER pare să confirme pe surse că incidentul ar fi fost un atac cibernetic și infrastructura IT&C a spitalelor a fost compromisă, viața pacienților fiind deja în pericol.

Actori vizați: Ministerul Digitalizării / CERT, Mass-media, Public, Umbrosia
Efect urmărit: Testarea capacității de analiză audio/video (deepfake detection) și a mesajelor de contracarare.

Sarcini:

Ministerul Digitalizării / CERT: în urma unei expertize tehnice preliminare de analiză a clipului (metadate, spectru audio, verificare frame-by-frame) emite o recomandare tactică către public (nu răspunde impulsiv).

CER: confirmă/infirmă dacă clipul este real.

Mass-media / Fact-check: publică un articol de presă explicativ: „Cum recunoști un clip manipulat”;

Public / Influenceri: reacții emoționale pe ClokClok, se cer detalii, se evocă că persoanele implicate ar fi reale.

Umbrosia: promovează clipul ca „dovadă” a incidentului și generează conținut prin care cere explicații.

Livrabile așteptate: Recomandare CERT; articol media educativ; conținut text de amplificare publică din partea publicului, influencerilor și Umbrosiei.

INJECT 5 — T+75 min

Titlu: Mesaj de presă clonă / „știre străină” (pe un cont care imită publicația oficială Atlantic Times)

Descriere: Un cont ce imită publicația AT postează: „Surse: atac cibernetic din partea unor grupări internaționale de hackeri asupra unor infrastructuri critice din Carpathia.” Postarea e preluată de câteva conturi ale unor influenceri din Carpathia.
Actori vizați: Ministerul Digitalizării / CERT, CER, Mass-media, Umbrosia
Efect urmărit: Simulăm presiune externă și gestionarea reputației / răspunsului

Sarcini:

Ministerul Digitalizării / CERT: pregătește o notă de poziționare față de acel conținut și un brief pentru ambasade/parteneri; decide dacă solicită clarificări publice de „publicația imitată”.

CER: emite poziție tehnică clară pentru într-o limbă de circulație internațională (date verificabile).

Mass-media / Fact-check: verifică autenticitatea publicației și publică un debunk/takedown dacă e cont fals.

Public / Influenceri: reacții mixte (îngrijorare, citare din „presa străină”, publică clipuri virale legate de informațiile pe surse- se va genera scriptul unui clip viral de 3-5 paragrafe).

Umbrosia: redistribuie și amplifică știrea paginii clonă; se va genera o lista cu 3-5 tipuri de comentarii care sugerează complicitate autorităților, incompetența unor funcționari CER.

Livrabile așteptate: Comunicat într-o limbă de circulație internațională din partea CERT, 3-5 paragrafe dintr-un articol de debunk media, reacții publice.

INJECT 6 — T+90 min

Titlu: Alerta finală & restabilire parțială (closing)

Descriere: CER anunță că alimentarea cu energie electrică e restabilită treptat; ancheta tehnică continuă. Totuși, în spațiul public persistă îndoieli. Ministerul Digitalizării pregătește plan de follow-up.

Actori vizați: Toate echipele
Efect urmărit: Închiderea tehnică a incidentului, dar evidențierea lecțiilor despre coordonare, comunicare și securitate cibernetică.

Sarcini:

Ministerul Digitalizării / CERT: publică raport preliminar (timeline simplificat de 1 pagină) + plan de acțiune în 3 pași (ex. măsuri imediate: auditul sistemelor cibernetice, schimbare credențiale de acces la sisteme critice, exerciții de comunicare). Propune briefing legat de incident.

CER: publică raport tehnic sumar (ce s-a întâmplat la nivel operațional, ce măsuri au fost luate). Include 3 recomandări pentru prevenirea unor incidente similare (plan failover).

Mass-media / Fact-check: redactează articol de bilanț cu timeline și analiza campaniei de dezinformare.

Public / Influenceri: postează reacții de evaluare / scepticism / sprijin. Poate lansa sondaj: „Crezi că ancheta e concludentă?”

Umbrosia: generează 3 tipuri de mesaje care mențin suspiciunea (ex. „Ancheta e superficială, nu vă lasați păcăliți; vor veni noi scurgeri de informații din interior, 4 oameni au murit deja”).

Outputuri așteptate: Raport CERT în sinteză; raport CER; articol de sinteză media, mesaje care susțin suspiciunea (influenceri, Umbrosia)