AMENINȚĂRILE HIBRIDE DIN PARTEA FEDERAȚIEI RUSE PE TERITORIUL UNIUNII EUROPENE

RUSSIAN HYBRID THREATS WITHIN THE EUROPEAN UNION MEMBER STATES

Maior dr. Sînziana IANCU*

Rezumat*: Conflictul contemporan depășește cadrul războiului convențional și integrează dimensiuni cibernetice, informaționale, cognitive, economice și spațiale într-un ecosistem de amenințări hibride aflat în continuă transformare. Granița dintre pace și război devine tot mai dificil de delimitat, iar actorii statali și non-statali folosesc instrumente de influență, dezinformare și atacuri cibernetice pentru a afecta procesele decizionale și infrastructurile critice. Lecțiile recente ale conflictelor moderne evidențiază rolul esențial al infrastructurilor digitale, comunicațiilor și sistemelor satelitare în securitatea națională și internațională.*

Dezvoltarea accelerată a tehnologiilor emergente, precum inteligența artificială, Internet of Things și calculul cuantic, amplifică atât oportunitățile, cât și vulnerabilitățile strategice. În acest context, reziliența devine un obiectiv central, bazat pe cooperarea dintre instituțiile statului, sectorul privat, mediul academic și societatea civilă. Consolidarea securității cibernetice, protejarea infrastructurilor critice, reducerea dependențelor tehnologice și intensificarea cooperării internaționale sunt considerate condiții esențiale pentru apărarea societăților democratice în fața amenințărilor hibride.

Cuvinte cheie**:** *război hibrid, securitate cibernetică, inteligență artificială, reziliență, infrastructuri critice.*

Abstract: *Contemporary conflict extends beyond conventional warfare, integrating cyber, informational, cognitive, economic, and space dimensions into an evolving ecosystem of hybrid threats. The boundary between war and peace is becoming increasingly blurred, as both state and non-state actors employ influence operations, disinformation campaigns, and cyberattacks to disrupt decision-making processes and target critical infrastructure. Recent conflicts have demonstrated the strategic importance of digital infrastructures, communication networks, and satellite systems in maintaining national and international security.*

The rapid development of emerging technologies, such as artificial intelligence, the Internet of Things, and quantum computing, creates both new opportunities and significant strategic vulnerabilities. In this context, resilience has become a central objective, requiring close cooperation among government institutions, the private sector, academia, and civil society. Strengthening cybersecurity, protecting critical infrastructure, reducing technological dependencies, and enhancing international cooperation are considered essential measures for safeguarding democratic societies against hybrid threats.

Keywords: *hybrid warfare, cybersecurity, artificial intelligence, resilience, critical infrastructure.*

* membru corespondent al Academiei de Științe ale Securității, ministru consilier în MAE, email: iancu_sanziana@yahoo.com

I. Introducere

Războiul contemporan nu mai poate fi înțeles exclusiv prin prisma confruntării militare convenționale, ci presupune integrarea simultană a dimensiunilor cibernetice, informaționale, cognitive, economice și spațiale într-un ecosistem de amenințări hibride aflat într-o continuă evoluție.

Granița tradițională dintre război și pace devine din ce în ce mai difuză. Actorii statali și non-statali utilizează instrumente hibride pentru a influența percepțiile, a vulnerabiliza societățile democratice și a afecta procesele decizionale fără a depăși pragul unui conflict armat declarat. În acest context, domeniul cibernetic a fost definit ca un „câmp de luptă invizibil", în care infrastructura digitală, rețelele de comunicații și spațiul informațional devin simultan ținte, arme și vectori de influență strategică.

Aproape orice conflict contemporan dezvoltă o componentă cibernetică proprie, iar operațiunile cibernetice sunt utilizate atât pentru spionaj și pre-poziționare strategică, cât și pentru sabotaj, coerciție, influențare informațională și afectarea infrastructurii critice. **Lecțiile desprinse din războiul din Ucraina reprezintă un punct de referință pentru înțelegerea modului în care infrastructurile energetice, comunicațiile satelitare, sistemele logistice și rețelele de comandă și control pot deveni ținte prioritare ale actorilor ostili.**

Un accent important a fost pus asupra relației dintre tehnologiile emergente și transformarea conflictului hibrid. Inteligența artificială, Internet of Things (IoT), calculul cuantic și tehnologiile XR/Metaverse sunt nu doar ca instrumente de progres tehnologic, ci și surse majore de vulnerabilitate strategică. Inteligența artificială accelerează semnificativ dezvoltarea operațiunilor de influență, generarea de conținut manipulator, automatizarea atacurilor de tip *phishing* și dezvoltarea de *malware* adaptativ. În același timp, tehnologiile cuantice generează riscul unor ***campanii de tip „harvest now, decrypt later"***, prin care datele criptate sunt culese în prezent, pentru a fi decriptate ulterior.

În ceea ce privește dimensiunea cognitivă a conflictului, spațiul informațional a devenit unul dintre principalele teatre ale confruntării strategice. Campaniile de dezinformare și operațiunile de tip FIMI urmăresc manipularea percepțiilor publice, polarizarea societăților și diminuarea încrederii în instituțiile democratice. În acest sens, s-a remarcat că inteligența artificială permite personalizarea și amplificarea mesajelor manipulatorii într-un ritm și la o scară fără precedent, transformând operațiunile informaționale într-un proces mult mai greu de detectat și atribuit.

Avem, totodată, de a face cu o **transformare a spațiului cosmic într-un nou domeniu al competiției hibride**. **Infrastructurile orbitale și sistemele satelitare sunt descrise drept „coloana vertebrală invizibilă" a economiei și securității globale**, deoarece susțin comunicațiile, navigația, sistemele financiare, operațiile militare și infrastructura critică modernă. În acest context, atacurile cibernetice și interferențele asupra sistemelor

spațiale sunt considerate capabile să producă efecte strategice majore asupra societăților contemporane.

Încă din doctrinele antice ale războiului, putem afla că atacul este adesea mai facil decât apărarea, iar astăzi, în spațiul cibernetic și spațial, cu atât mai mult, mai ales prin dificultatea atribuirii responsabilității care favorizează desfășurarea operațiunilor sub pragul conflictului convențional. **Conceptul de „plausible deniability" a devenit, în ultimii ani, una dintre caracteristicile definitorii ale războiului hibrid modern, actorii ostili utilizând frecvent *structuri proxy*, *grupări hacktiviste* sau companii private pentru mascarea implicării directe.**

În plan operațional și doctrinar, a fost evidențiat rolul tot mai important al cooperării internaționale și al structurilor euro-atlantice în dezvoltarea rezilienței cibernetice. În același timp, de ajutor sunt și exercițiile internaționale întrunite, mecanismele de cooperare și inițiativele doctrinare destinate integrării capabilităților cibernetice în planificarea operațională modernă. Spațiul cibernetic este tratat, în prezent, ca domeniu operațional distinct, alături de domeniile terestru, aerian, maritim și spațial, iar securitatea informației este considerată o componentă esențială a securității colective. În acest context mai amplu, se observă relevanța crescândă a unor inițiative precum **Foreign Information Manipulation and Interference Information Sharing and Analysis Center (FIMI-ISAC)**, o rețea internațională dedicată protejării societăților democratice împotriva manipulării informaționale și ingerințelor străine. Astfel de inițiative facilitează schimbul de informații, dezvoltarea unei imagini comune de situație și coordonarea răspunsurilor între guverne, societatea civilă, mediul academic și sectorul privat în fața unor operațiuni de influență tot mai sofisticate.

Dezbaterile privind reziliența națională au evidențiat importanța cooperării dintre stat și sectorul privat în protejarea infrastructurilor critice. În majoritatea statelor occidentale, infrastructura digitală și energetică sunt operate, în principal, de companii private, ceea ce transformă cooperarea interinstituțională și schimbul de informații într-o condiție fundamentală pentru apărarea cibernetică eficientă. În acest sens, modelele nordice de reziliență sunt exemple relevante de integrare a culturii de securitate la nivel societal, bazate pe încredere, cooperare și pregătire continuă.

În același timp, utilizarea instrumentelor diplomatice în răspunsul la amenințările cibernetice externe este un instrument semnificativ în determinarea cel puțin a unei soluții defensive. Atribuirea publică a atacurilor, sancțiunile și cooperarea internațională sunt alte instrumente capabile să reducă spațiul de manevră al actorilor ostili și să contribuie la descurajarea operațiunilor hibride.

Vulnerabilitățile generate de dependențele tehnologice și de lanțurile globale de aprovizionare reprezintă întotdeauna un subiect important de discuție la nivel regional și global, cu precădere în contextul actual al intensificării majore a amenințărilor de tip hibrid, pe fondul războiului din proximitate, dar și al altor conflicte cu impactul bulgărelui de zăpadă. În

prezent, adeseori, sunt formulate preocupări privind utilizarea pe scară largă a echipamentelor și componentelor digitale produse de actori externi, precum și riscurile asociate actualizărilor de *firmware*, culegerii datelor operaționale și accesului persistent în rețele critice. Astfel, **securitatea lanțurilor de aprovizionare și reducerea dependențelor strategice au fost definite drept priorități esențiale pentru statele democratice**.

Războiul hibrid exploatează în mod sistematic decalajele dintre ritmul dezvoltării tehnologice și capacitatea instituțiilor democratice de adaptare. Actorii ostili operează într-o zonă gri („*grey zone*") caracterizată prin ambiguitate juridică, dificultăți de atribuire și fragmentare instituțională, profitând de lipsa interoperabilității și de întârzierile proceselor decizionale.

În acest context, conceptul de reziliență este definit într-o manieră extinsă, depășind dimensiunea strict tehnică sau militară. Reziliența presupune capacitatea societăților de a absorbi șocurile, de a continua funcționarea instituțională și de a reveni rapid la normalitate în urma unor atacuri hibride. În acest fel, putem vorbi despre o *abordare de tip „whole of society"*, bazată pe cooperarea permanentă dintre instituțiile statului, sectorul privat, mediul academic și societatea civilă.

Tehnologia redefinește profund natura conflictului contemporan și infrastructura digitală, spațiul informațional și dimensiunea cognitivă reprezentând componente centrale ale securității internaționale. Într-un mediu strategic caracterizat de competiție permanentă, atacuri hibride și accelerare tehnologică, adaptarea instituțională rapidă, dezvoltarea culturii de securitate și consolidarea cooperării internaționale condiționează protejarea rezilienței democratice și a securității colective.

II. Tehnici, tactici și proceduri ale amenințărilor hibride din partea Federației Ruse

Asistăm astăzi la o confruntare escaladată între strategiile de prezervare a identității naționale și factorii externi tot mai agresivi față de ordinea și stabilitatea mediului de securitate. Toate acestea se întâmplă pe fondul unor activități hibride persistente și adaptative desfășurate de F. Rusă împotriva societăților democratice occidentale. F. Rusă utilizează din ce în ce mai frecvent agenți de unică folosință (***single-use agents***), rețele criminale și actori non-statali pentru desfășurarea unor operațiuni cu grad ridicat de negare (***plausible deniability***) în exterior. Potrivit unor autori, în ultimul an, au fost identificați peste 100 de indivizi implicați în activități asociate operațiunilor ruse de influență sau destabilizare în state occidentale, majoritatea având antecedente penale și peste 600 de operativi ruși au fost expulzați din statele europene pro-occidentale, începând cu 2018[1].

[1] Kacper Rekawek et al, *Russia's Crime–Terror Nexus Criminality as a Tool of Hybrid Warfare in Europe*, Septembrie 2025, disponibil la https://www.globsec.org/sites/-default/files/202510/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf, accesat la 30 Mai 2026, p. 06.

Rusia promovează o „legătură *fantomă*-gangster", în care actorii din domeniul securității statului funcționează ca filiale ale elitelor criminale („fantome"), care subcontractează sarcini către „gangsteri" sau entități care operează în afara controlului formal al statului.[2]

Federația Rusă a recrutat deja mii de condamnați pentru efortul său de război din Ucraina. Dovezile sugerează că metode similare sunt aplicate operațiunilor hibride din Europa. Închisorile, atât în F. Rusă, cât și în străinătate, oferă rezerve de recruți legați de crima organizată și obișnuiți cu violența. Acest lucru reflectă practicile anterioare ale unor grupări, precum ISIS, care tratau sistemele penale ca rezervoare de agenți pentru violența politică[3].

Moscova începe adesea cu infractori mărunți (hoți, traficanți de droguri sau persoane îndatorate), al căror rol inițial este limitat la acte de nivel scăzut. Cu toate acestea, recrutarea repetată poate determina acești actori să construiască grupuri criminale mai structurate. Aceste grupuri pot apoi evolua în rețele organizate care servesc interesele Moscovei mai sistematic, alimentând „legătura mai largă dintre *fantome* și gangsteri" și permițând potențial atacuri mai sofisticate sau mai mortale[4].

Privind retrospectiv, numai în 2025, autoritățile de securitate din Germania au înregistrat 320 de tentative de sabotaj suspectate, însă atribuirea clară rămâne dificilă, deoarece autorii sunt rareori identificați.[5] Referitor la distribuția geografică a incidentelor, mai mult de un sfert din incidentele nou identificate (11 în perioada iulie 2025 și februarie 2026, raportat la februarie 2022 și februarie 2026), au avut loc în Polonia, care era deja țara cea mai frecvent vizată. Cu 31 de incidente în total, Polonia se remarcă acum și mai clar ca principalul focar al activității rusești[6]. Creșteri semnificative au fost observate și în Franța, care a înregistrat cinci cazuri noi și acum se situează la 20 de incidente în total (2022 – 2026), ceea ce o face a doua cea mai afectată țară. Lituania și Germania înregistrează acum fiecare câte 15 incidente, urmate de Regatul Unit cu 12 și Estonia cu 11. Această distribuție sugerează cu tărie că sprijinul pentru Ucraina este cel mai important factor care modelează selecția țintelor. Unii dintre cei mai pronunțați susținători ai Ucrainei, cum ar fi Polonia, Franța, Germania și Regatul Unit, reprezintă împreună mai mult de jumătate din toate incidentele identificate. În plus, statele baltice, denumite derogatoriu ca parte a unei „externe apropiate" mai largi de către F. Rusă, reprezintă aproape o cincime din toate cazurile înregistrate.

[2] *Ibidem*, p. 13.
[3] *Ibidem*, p. 4.
[4] *Ibidem*, p. 31.
[5] Julian Lanchès, Kacper Rekawek, *More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited*, 23 Feb. 2026, disponibil la https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited, accesat la 30 Mai 2026.
[6] *Ibidem*.

Exemple de astfel de cazuri[7]:

* septembrie 2025: 11 persoane sârbe au fost arestate în Serbia. Acestea călătoriseră anterior, adesea în constelații diferite, prin Europa și erau asociate cu mai multe incidente care vizau incitarea la polarizare etnică și rasială (turnarea de vopsea verde peste situri evreiești din Paris și din împrejurimi, amplasarea de schelete cu inscripții la Poarta Brandenburg, lipirea de autocolante cu mesaje genocidale în zona mai largă a Parisului, depunerea de capete de porc tăiate în fața moscheilor din oraș și din împrejurimi). Autoritățile franceze au conectat activitățile lor de interferența străină a unui actor statal ostil, și anume Federația Rusă[8].

* octombrie 2025: autoritățile române și poloneze, într-o acțiune comună, au dejucat comploturi de trimitere a explozibililor prin Polonia și România către Ucraina. Mai exact, planul implica expedierea a două colete incendiare prin intermediul Nova Poshta, o companie de curierat ucraineană care operează între statele membre UE și Ucraina. Dispozitivele ar fi fost destinate să aprindă și să distrugă clădirea companiei de curierat din centrul Bucureștiului. Un cetățean ucrainean, Vitalij S., a fost arestat în Polonia, în timp ce România a reținut alți doi cetățeni ucraineni anonimi[9].

* octombrie 2025: Patru bărbați ruși cu vârste cuprinse între 26 și 38 de ani, din Daghestan, au fost arestați în Franța sub suspiciunea de complot pentru asasinarea disidentului rus Vladimir Osechkin, fondatorul unei organizații (*Gulagu.net*) pentru drepturile omului. Se pare că cei patru călătoriseră deja la începutul anului 2025 la reședința lui Osechkin din Franța pentru a efectua supravegheri. Una dintre persoane deținea și cetățenie franceză[10].

* noiembrie 2025: autoritățile franceze au arestat trei persoane în cadrul unei anchete privind o asociație franco-rusă suspectată de răspândirea propagandei Kremlinului și culegerea de informații în interesul F. Ruse. Un bărbat rus în vârstă de 40 de ani, a fost surprins pe imaginile de supraveghere ale orașului, lipind postere pro-ruse pe Arcul de Triumf din Paris și raportând apoi șefului asociației (*SOS Donbass*)[11].

* noiembrie 2025: trei ucraineni au aruncat în aer șine de cale ferată în estul Poloniei cu scopul de a deraia trenuri, unul dintre ei fiind la un pas de fragmentul distrus al șinelor. Autorii au intrat în Polonia special pentru a comite atacul și s-au întors, ulterior, în Belarus. Potrivit informațiilor, unul dintre autori avea o relație de mai lungă durată cu serviciile de informații rusești și fusese implicat anterior într-un atac eșuat cu explozibili împotriva unei fabrici din Ucraina[12].

Această tendință reflectă preferința Moscovei pentru utilizarea intermediarilor și a structurilor proxy, care permit statului rus să își

[7] *Ibidem.*
[8] *Ibidem.*
[9] *Ibidem.*
[10] *Ibidem.*
[11] *Ibidem.*
[12] *Ibidem.*

mascheze implicarea directă, exploatând, în același timp, vulnerabilitățile populației.

Din cei 131 de autori identificați, 62% au comis atacuri multiple, iar 89% au acționat în grupuri de cel puțin doi. 93% dintre autori erau bărbați, cu vârsta medie de 30 de ani, provenind dintr-o țară post-sovietică, motivați de compensații financiare[13]. Doar 58% dintre autori știau că activitățile lor erau dirijate de serviciile rusești. 27% dintre autori aveau cazier judiciar sau implicare anterioară în activități ilicite.[14]

Populația generală devine adesea un instrument indirect al operațiunilor hibride, fără a conștientiza obiectivele strategice reale din spatele propriilor acțiuni. Cu alte cuvinte, indivizii nu ajung să conștientizeze sau să afle că rezultatul propriilor lor acțiuni este capitalizat de F. Rusă, deoarece sunt folosite terțe elemente (proxy). Prin exploatarea diviziunilor sociale, a ecosistemelor online de influență, a intermediarilor locali, actorii ruși urmăresc amplificarea polarizării și erodarea încrederii în instituțiile democratice. Incidentele recente privind incursiuni cu drone în proximitatea aeroporturilor și a infrastructurii critice ilustrează, de asemenea, comportamentul tot mai vizibil și mai agresiv adoptat de Federația Rusă, precum și faptul că niciun stat nu este imun la asemenea provocări.

Cu privire la comunicarea strategică rusă, aceasta a devenit semnificativ mai explicită și coercitivă. Spre deosebire de perioadele anterioare, caracterizate prin ambiguitate și semnalizare indirectă, actorii ruși au început recent să publice liste cu potențiale viitoare ținte. Această evoluție sugerează o normalizare graduală a practicilor de intimidare în cadrul spectrului hibrid. În acest context, apar întrebări fundamentale referitoare la definirea „liniilor roșii" strategice și la riscul acceptării activităților hibride ostile drept parte a unui așa-numit „nou normal" - ***This is the new normal, but don't get used to it*** - în ideea că ar trebui să căutăm în continuare soluții și strategii de estompare a acestor amenințări, de acum directe, venite din partea Federației Ruse. Deși tacticile, tehnicile și procedurile (TTPs) rămân în mare parte similare, amploarea și vizibilitatea acestor operațiuni s-au intensificat considerabil.

II. 1. Amenințările hibride ruse în zona electorală

Tentativele Federației Ruse de influențare a procesului politic din R. Moldova (inclusiv în contextul alegerilor prezidențiale din 2024 și al alegerilor parlamentare din 2025) fac din aceasta un posibil teren de testare pentru viitoare operațiuni rusești de interferență electorală în alte state europene. Astfel, este posibil ca aceste campanii rusești de interferență electorală să fie pregătite în avans, de regulă, cu cel puțin șase luni înainte,

[13] Kacper Rekawek et al, *Russia's Crime–Terror Nexus Criminality as a Tool of Hybrid Warfare in Europe*, September 2025, disponibil la https://www.globsec.org/-sites/default/files/202510/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf, accesat la 30 Mai,2026, p. 23.
[14] *Ibidem*, p. 24.

necesitând resurse financiare consistente, pregătire logistică, rețele de influență și operațiuni informaționale coordonate. În acest sens, este posibil ca într-o fază preliminară, cu șase până la 12 luni înainte, să fie identificate vulnerabilitățile societății-țintă și creată infrastructura digitală și proxy, folosindu-se sume importante de bani și operațiuni cibernetice complexe. Cu aproximativ trei până la șase luni înainte, pot apărea operațiunile de influență, prin care se activează rețelele de influență (precum boți, ferme de troli și canale media proxy) pentru a polariza electoratul, urmând ca lovitura de grație (ultima fază) să aibă loc în ultimele săptămâni, prin mesaje puternic denigratoare și chiar Black Swan-uri.

Alegerile prezidențiale din octombrie-noiembrie 2024 și referendumul privind aderarea la UE din Republica Moldova au relevat o escaladare semnificativă a operațiunilor FIMI ale Federației Ruse în țară, pe măsură ce activitățile s-au intensificat ca răspuns la aspirațiile R. Moldova față de UE[15]. În lunile premergătoare alegerilor, Federația Rusă a utilizat o infrastructură FIMI complexă, multistratificată și adaptivă. Aceste operațiuni au combinat strategic infrastructura existentă cu active nou dezvoltate pentru a manipula opinia publică, a destabiliza procesul electoral și a submina procesul de extindere a UE în regiune[16].

De aceea, păstrarea unei vigilențe continue este esențială, precum și menținerea finanțării măsurilor de contracarare la nivel național și european și a dezvoltării unor mecanisme credibile de descurajare.

Câteva exemple de dezinformare pe acest palier[17]:

*** Estonia:** În timpul alegerilor, o afirmație falsă s-a răspândit pe rețelele sociale, sugerând că alegătorii ar trebui să aducă propriile pixuri la secțiile de votare, deoarece cele oferite erau „ștergătoare" și ar putea altera voturile[18];

*** Franța:** Anterior alegerilor prezidențiale, grupuri extremiste din Franța au răspândit dezinformări împotriva vaccinării și restricțiilor COVID-19, promovând teorii ale conspirației pentru a crea neîncredere în instituții[19];

*** Germania:** În Germania, grupurile de extremă dreaptă au propagat narațiuni despre fraude electorale, preluate de la mișcările de negare a alegerilor din SUA, pentru a submina procesele democratice[20];

---

[15] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 29 in chapter "Exposing the architecture of FIMI operations: a network analysis of influence operations", Martie 2025, disponibil la https://www.eeas.europa.eu/-sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?, accesat la 26 Mai 2026.

[16] *Ibidem*.

[17] Igor Soroceanu, *Dezinformarea în campaniile electorale*, 02nd of May, 2025, disponibil la https://revista.universuljuridic.ro/dezinformarea-in-campaniile-electorale/, accesat la 30 Mai 2026.

[18] *Ibidem.*

[19] *Ibidem.*

[20] *Ibidem.*

* **Slovacia:** Campaniile de dezinformare din Slovacia au inclus clipuri audio generate de inteligența artificială, în care lideri politici păreau să discute despre manipularea alegerilor. Acestea au fost distribuite pe scară largă înainte de a fi dezmințite[21];
* **Spania:** În alegerile din 2023, au circulat narațiuni false despre interferențe străine și fraude electorale, incluzând afirmații că oficialii UE făceau campanie pentru anumiți candidați[22].

Chiar dacă impactul dezinformării variază de la o țară la alta, răspândirea rapidă a acestui fenomen, dezvoltarea sa tehnică, incluzând viteza, amploarea și extrateritorialitatea, percepția sa inofensivă de către societate și cerințele sale de finanțare relativ limitate constituie schimbări și amenințări majore, nu numai pentru procesul electoral, dar și pentru democrații, în general[23].

În 2024, Federația Rusă a folosit aceste tactici manipulatoare în special în contextul alegerilor europene, unde organizațiile pro-Kremlin au încercat să vizeze alegătorii din statele membre ale UE cu narațiuni care subminează sprijinul pentru Ucraina. Alte elemente semnificative includ campanii de denigrare a liderilor politici europeni proeminenți cu acuzații de corupție și încercări de a alimenta protestele, de a încuraja abținerea de la vot și de a incita neîncrederea în instituțiile europene[24]. Cu toate acestea, UE și statele sale membre au observat în mod corespunzător aceste încercări de manipulare și au contracarat afirmațiile false prin campanii de expunere și conștientizare. EuvsDisinfo a publicat în mod activ analize care expun operațiunile FIMI care vizează influențarea alegerilor[25]. Mai mult, campaniile FIMI ale Federației Ruse au căutat, de asemenea, să exploateze vulnerabilități locale specifice în sferele politice, sociale și tehnologice cu conținut atent adaptat și țintit, în special acolo unde Federația Rusă urmărește să își promoveze interesele de politică externă și de securitate[26]. În 2024, Federația Rusă a încercat, de asemenea, să se amestece în procesele democratice din Moldova, vizând atât alegerile prezidențiale, cât și referendumul privind aderarea la UE.

Per ansamblu, rolul Federației Ruse ca actor FIMI reflectă modul în care aceasta percepe spațiul informațional ca pe un domeniu de luptă. Folosind o combinație de actori statali și nestatali, Federația Rusă a dezvoltat o strategie cu mai multe straturi și a căutat să modeleze narațiuni

[21] *Ibidem.*
[22] *Ibidem.*
[23] *Ibidem.*
[24] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 12 în cap. "FIMI trends and findings in 2024", subcapitol "Russia as a FIMI threat actor in 2024", Martie 2025, disponibil la https://www.eeas.europa.-eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?, accesat la 26 Mai 2026.
[25] *Ibidem.*
[26] *Ibidem.*

globale pentru a promova obiectivele geopolitice ale Moscovei[27]. Concentrându-se pe exercitarea unei influențe pe termen lung, mai degrabă decât pe incidente izolate, Federația Rusă continuă să exploateze punctele slabe din peisajul informațional global, ceea ce face ca tacticile sale FIMI să fie o problemă serioasă de securitate pentru UE[28]. Invazia la scară largă a Ucrainei de către Federația Rusă din 24 februarie 2022 a evidențiat spectrul larg de tactici de manipulare a informațiilor utilizate de acest actor statal.

Patru elemente-cheie au definit operațiunile Federației Ruse[29]: * În primul rând, utilizarea simultană a canalelor secrete și publice, abandonând discreția anterioară și făcând eforturile sale de influență mai vizibile. * În al doilea rând, canalele oficiale rusești și mass-media controlată de stat și-au intensificat rolul, sporindu-și prezența și promovând narațiuni mai agresive vizând Moldova. * În al treilea rând, infrastructura rusească FIMI utilizată anterior împotriva Ucrainei a fost redistribuită pentru a ataca R. Moldova, adaptând rețelele și narațiunile la un nou front de interferență. * În al patrulea rând, o rețea de noi canale locale a acționat ca o coloană vertebrală pentru distribuirea conținutului, asigurându-i rezonanța și credibilitatea în rândul publicului local și permițând extinderea sa în spațiul mass-media. Operațiunile rusești de influență sunt coordonate printr-un ecosistem complex care include criptomonede, oligarhi locali, influenceri, bloggeri, grupări de huligani și chiar structuri religioase[30].

II.2. Amenințările hibride ruse în zona religioasă

De multe ori, au fost observate activități asociate Bisericii Ortodoxe Ruse, a cărei influență ar fi fost extinsă deliberat în anumite state ca parte a unor campanii mai ample de influență strategică.

Asemenea exemple au fost observate în Europa de Nord, astfel:

*** Suedia**[31]: În orașul Västerås (100 km V Stockholm), autoritățile au închis o structură asociată Bisericii Ortodoxe Ruse pe fondul suspiciunilor privind activități de spionaj. Autoritățile suedeze au demascat călugărițe de la Mănăstirea "Sfânta Elisabeta" din Belarus, suspectate de colaborare cu serviciile de informații militare ruse. Conform anchetei, acestea au operat ani de zile în țările UE sub pretextul activităților religioase, au strâns fonduri din vânzarea de produse religioase și le-au transferat pentru nevoile armatei

[27] *Ibidem.*
[28] *Ibidem*.
[29] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 29 in chapter "Exposing the architecture of FIMI operations: a network analysis of influence operations", Martie 2025, disponibil la https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?, accesat la 26 Mai 2026.
[30] *Ibidem*.
[31] Roméo Langlois et. al., *Exclusive investigation: Is the Russian Orthodox Church in Sweden a platform for espionage?*, 07th of April, 2025, disponibil la https://www.france24.com/en/tv-shows/reporters/20250704-exclusive-investigation-is-the-russian-orthodox-church-in-sweden-a-platform-for-espionage, accesat la 26 Mai 2026.

ruse și au vizitat teritorii ocupate temporar în Ucraina. În iarna anului 2025, acestea au venit în Suedia pentru a-și continua activitățile. La acea vreme, protopopul Andrei Lemeșonok a numit deschis mănăstirea sa „unitate de luptă" în războiul împotriva Ucrainei[32]. Acest caz demonstrează clar că F. Rusă folosește Biserica Ortodoxă Rusă ca instrument de influență hibridă. Sub pretextul religiei, acestea culeg informații, răspândesc propagandă pro-rusă, legitimizează agresiunea împotriva Ucrainei și creează rețele de influență asupra societăților occidentale[33]. Îngrijorarea s-a concentrat și pe **amplasarea sensibilă a bisericii**, foarte aproape de un aeroport important din punct de vedere strategic, de o stație de tratare a apei și de companii energetice avansate cu sediul în orașul Västerås, cu 130.000 de locuitori, situat la doar 100 de kilometri vest de Stockholm[34].

*** Norvegia[35]:** Mai multe entități religioase de pe teritoriul său se află în **apropierea unor locații strategice**. Serviciul de Securitate al Poliției din Norvegia (PST) nu a detaliat public cazurile, dar analize independente arată o geografie izbitoare a bisericilor și capelelor ortodoxe din Norvegia, aliniate cu patriarhatul Moscovei, amplasate în apropierea unor situri militare, industriale sau guvernamentale[36]: *Oslo - Parohia "Sfânta Prințesă Olga", care funcționează în capitală din 2003, se află în districtul central, la doar câteva sute de metri de principalele facilități guvernamentale. Pe o rază de 1 km de biserică se află Parlamentul Norvegiei (Stortinget), Biroul de Statistică (SSB), mai multe ministere și cel puțin șapte ambasade străine; * Bryne - Biserica "Sfânta Muceniță Irina", construită în 2014, în mijlocul unui grup de firme de producție de înaltă tehnologie. Pe o rază de 800 m de biserică se află companii specializate în prelucrarea metalelor avansate, automatizare robotică și componente semiconductoare, inclusiv *Nordic Steel AS* (la 650 m distanță) și *IXYS Norway*, la aproximativ 586 m distanță. Astfel de firme aprovizionează sectoarele energetic și ingineresc din Norvegia, iar apropierea lor de o parohie rusă înființată după 2014 ridică semnale de alarmă; * Kirkenes - Parohia "Sfântul Trifon din Pechenga" funcționează din 2015 în orașul de frontieră Kirkenes (granița de nord-est a Norvegiei cu F. Rusă). Această zonă prezintă un interes strategic deosebit: biserica se află la doar 5 km de Garnizoana Sør-Varanger (care păzește granița NATO – Federația Rusă) și se află la câteva sute de metri de

[32] Center for countering disinformation, *In Sweden nuns were exposed for spying for Russian intelligence*, 19th of January, 2026, disponibil la https://cpd.gov.ua/en/international-threats-en/europe/in-sweden-nuns-were-exposed-for-spying-for-russian-intelligence/, accesat la 26 Mai 2026.

[33] *Ibidem*.

[34] Charlie Duxbury, *New Russian church raises suspicions in Swedish town*, 11th November, 2024, disponibil la https://www.politico.eu/article/new-russian-orthodox-church-suspicion-sweden-town-vasteras/, accesat la 26 Mai 2026.

[35] Nordic Defence Review, *Russian Orthodox Churches in Europe: Espionage Outposts Under the Guise of Faith*, s.a., disponibil la https://nordicdefencereview.com/russian-orthodox-churches-in-europe-espionage-outposts-under-the-guise-of-faith/, accesat la 30 Mai 2026.

[36] *Ibidem*, accesat la 26 Mai 2026.

birourile municipalității locale și de Consulatul General al Rusiei; * Vardø - o capelă ortodoxă rusă, în construcție din 2017 până recent, aflată pe o insulă arctică îndepărtată din Vardø, nu departe de instalația radar GLOBUS. Se crede că radarul din Vardø, operat de serviciile secrete norvegiene cu sprijinul SUA, alimentează și sistemul de apărare antirachetă al NATO, ceea ce îl face unul dintre cele mai bine păzite active ale Norvegiei; * Trondheim - Parohia "Sfânta Ana din Novgorod", construită în 2008, la o distanță de aprox.1 km de mai multe instalații de apărare, inclusiv un buncăr pentru submarine, o academie a forțelor aeriene și instalații militare, fiind și în proximitatea portului naval al orașului, respectiv a unor consulate ale țărilor NATO (printre care cele ale Finlandei, Poloniei, Danemarcei și Olandei). O astfel de locație ar putea oferi unui „enoriaș" atent oportunități ample de a observa mișcările militare. Pe teritoriul norvegian, acest model reflectă întocmai experiența Suediei, prin existența unor lăcașe de cult în zone de importanță strategică. Este grăitor faptul că personalități religioase rusești din Norvegia, precum părintele Khukhtamyaki și alții, au legături directe cu Patriarhul Kirill și au urmat în mare măsură linia politică a Moscovei[37].

*** Finlanda[38]:** În august 2022, autoritățile din orașul Turku au închis parohia ortodoxă rusă locală – Biserica "Adormirii Maicii Domnului", invocând invazia Federației Ruse în Ucraina drept motiv. Acesta a fost un pas remarcabil: evacuarea efectivă a unei biserici legate de Moscova, pe fondul temerilor că ar putea amenința securitatea națională. Locația parohiei din Turku era cu siguranță evidentă. Aceasta se afla lângă baza navală Pansio, unde se află flota de coastă a Finlandei, nu departe de portul Turku și în apropierea primăriei și a sediului Administrației Regionale de Stat și în proximitatea Consulatului General al Federației Ruse. Cu alte cuvinte, un avanpost religios rusesc poziționat în aceeași vecinătate cu o instalație navală finlandeză și misiunea diplomatică a Federației Ruse.

În capitala Helsinki, Parohia "Sfântul Nicolae Făcătorul de Minuni", activă din 1938, se află pe o rază de 3 km de cel puțin șase instalații militare sau maritime și de mai multe birouri guvernamentale. De asemenea, o altă capelă a Bisericii Ortodoxe Ruse, de dimensiuni mai reduse, construită în 2000 în estul Helsinki, se află în apropierea portului comercial Vuosaari și a unei centrale electrice majore.

*** Olanda[39]:** În Haga, Biserica Ortodoxă Rusă a deschis o mănăstire de călugări în 1972 (Mănăstirea "Sfântul Ioan Botezătorul"), care a funcționat discret timp de decenii. După invazia Federației Ruse, însă, autoritățile și jurnaliștii olandezi au început să observe că mănăstirea se afla într-un grup dens de facilități guvernamentale și legate de apărare. Nu mai puțin de 29 de birouri guvernamentale se aflau în vecinătatea sa, inclusiv sediul Federației Asociațiilor Europene de Tehnologie a Apărării (la doar ~400 m distanță) și o instalație a Armatei Olandeze (la ~2 km distanță).

[37] *Ibidem.*
[38] *Ibidem*, accesat la 30 Mai 2026.
[39] *Ibidem.*

Portul exterior și o centrală electrică importantă se aflau, de asemenea, la câțiva kilometri. Într-o atmosferă de neîncredere crescândă, mănăstirea de la Haga s-a închis în decembrie 2022, la scurt timp după începerea războiului.

În orașul portuar Rotterdam, Biserica Ortodoxă Rusă a construit biserica "Sfântul Alexandru Nevski", în 2004, cu implicarea unei firme de construcții rusești și a fost sfințită personal de Patriarhul Kirill, pe atunci Mitropolit. Biserica din Rotterdam se află în mijlocul unei infrastructuri critice: aproximativ nouă clădiri guvernamentale, inclusiv Parchetul din Rotterdam (la puțin peste 1 km distanță), se află în apropiere. Conform rapoartelor de investigație, pe o rază de 3-4 km de biserică se află, de asemenea, două instalații militare, un centru logistic maritim și un furnizor de echipamente pentru centrale electrice. În plus, Rotterdam găzduiește o parohie mai veche, din 1959, care este, de asemenea, situată în apropierea unei infrastructuri importante.

*** Cehia[40]:** În Praga, istorica "Catedrală a Sfinților Chiril și Metodie", care aparține Bisericii Ortodoxe Cehe și Slovace, a primit finanțare substanțială pentru restaurări de la Gazprom Neft, compania petrolieră de stat rusă. Arhiepiscopul Praghei a acordat o medalie unui consilier Gazprom Neft în semn de mulțumire pentru asistența acordată catedralei. Această legătură financiară evidentă cu ramura energetică a Kremlinului a declanșat semnale de alarmă. Legislatorii din Praga au început să se întrebe de ce o companie de stat rusă era atât de interesată de o biserică cehă și ce influență ar putea aduce acest lucru. Îngrijorarea lor face parte dintr-o tendință mai largă: autoritățile cehe au „strâns șuruburile" împotriva entităților legate de Federația Rusă de când s-a aflat că agenții GRU ruși au aruncat în aer depozite de muniții pe teritoriul ceh în 2014.

În Moravia, Catedrala Ortodoxă din Gorazd, Olomouc, se află la aproximativ 70 km de locul exploziilor de la depozitul de muniții Vrbětice din 2014, un sabotaj orchestrat de agenți ruși. Deși această distanță este considerabilă, coincidența subliniază modul în care siturile Bisericii Ortodoxe Ruse au apărut chiar și în regiunile atinse ulterior de agresiunea secretă rusă.

În satul rural Vrbětice, o mică capelă ortodoxă, Capela "Treimii Dătătoare de Viață", există la aproximativ 72 km de fostul depozit, servind ca o amintire a prezenței religioase rusești în zonă. Anchetatorii cehi examinează dacă aceste facilități religioase și alte facilități religioase legate de Moscova ar fi putut facilita activități de spionaj sau subversiune rusească înainte sau după acel atac notoriu.

*** Bulgaria[41]:** Autoritățile bulgare au expulzat trei preoți ai Bisericii Ortodoxe Ruse (doi belaruși, unul rus) în 2022, din motive de securitate națională.

*** Estonia[42]:** Guvernul estonian a refuzat recent să reînnoiască permisul de ședere al conducătorului Bisericii Ortodoxe locale afiliate

[40] *Ibidem.*
[41] *Ibidem.*
[42] *Ibidem.*

Moscovei, invocându-l drept un risc de securitate din cauza justificării sale evidente a războiului Federației Ruse și a probabilelor legături cu serviciile religioase ale Moscovei.

La nivel paneuropean, instituțiile au început să reacționeze: în octombrie 2024, Consiliul Europei a mers până la a eticheta Biserica Ortodoxă Rusă drept un instrument de influență al Kremlinului, parte a unei rezoluții care i-a sancționat și pe propagandiștii ruși.[43]

* **Letonia:** A adoptat măsuri legislative și economice ferme pentru limitarea influenței ruse, inclusiv restricții privind deținerea terenurilor de către cetățeni ruși și extinderea sancțiunilor împotriva rețelelor proxy și a intermediarilor ruși.

Actuala confruntare cu Federația Rusă nu trebuie interpretată drept o anomalie temporară, ci ca expresie a modului în care Kremlinul percepe ordinea internațională și raporturile de putere. Din această perspectivă, așteptările privind o normalizare rapidă a relațiilor cu Federația Rusă pot fi considerate nerealiste pe termen scurt și mediu.

III. Concluzii

Analiza evoluției conflictului contemporan evidențiază faptul că războiul hibrid a devenit una dintre principalele forme de manifestare a competiției strategice dintre state, depășind cadrul tradițional al confruntării militare. Dimensiunile cibernetică, informațională, cognitivă și spațială sunt astăzi integrate într-un ecosistem complex de amenințări care exploatează vulnerabilitățile tehnologice, instituționale și sociale ale statelor democratice. În acest context, infrastructurile digitale, sistemele satelitare și spațiul informațional au dobândit o importanță strategică comparabilă cu cea a domeniilor operaționale clasice, iar capacitatea de adaptare la noile forme de conflict reprezintă o condiție esențială pentru menținerea securității naționale și colective.

Exemplele analizate demonstrează că Federația Rusă utilizează o gamă largă de tehnici, tactici și proceduri hibride, bazate pe utilizarea actorilor proxy, a rețelelor criminale, a operațiunilor de influență și a campaniilor de manipulare informațională. Aceste activități urmăresc erodarea încrederii în instituțiile democratice, amplificarea polarizării sociale și afectarea proceselor decizionale, inclusiv în perioade electorale. Totodată, utilizarea unor structuri aparent non-politice, inclusiv organizații religioase sau entități asociate acestora, evidențiază caracterul multidimensional și adaptativ al strategiilor de influență promovate de Moscova. Dificultatea atribuirii responsabilității și utilizarea sistematică a conceptului de „plausible deniability" permit desfășurarea unor astfel de operațiuni sub pragul conflictului convențional, complicând semnificativ răspunsul statelor vizate.

În fața acestor provocări, consolidarea rezilienței societale trebuie să depășească abordările strict militare sau tehnice și să adopte o perspectivă

[43] *Ibidem.*

integrată, de tip „whole of society”. Cooperarea dintre instituțiile statului, sectorul privat, mediul academic și societatea civilă, alături de dezvoltarea culturii de securitate, protejarea infrastructurii critice și intensificarea cooperării internaționale, reprezintă elemente fundamentale pentru contracararea amenințărilor hibride. În același timp, experiențele recente demonstrează că vigilența strategică, adaptarea continuă și dezvoltarea unor mecanisme eficiente de descurajare vor rămâne esențiale într-un mediu de securitate caracterizat de competiție permanentă, accelerare tehnologică și manifestarea tot mai agresivă a instrumentelor hibride de influență și destabilizare.

BIBLIOGRAFIE

3rd EEAS REPORT ON FOREIGN INFORMATION MANIPULATION AND INTERFERENCE THREATS, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 29 în cap. “Exposing the architecture of FIMI operations: a network analysis of influence operations”, Martie 2025, disponibil la https://www.eeas.europa.eu/sites/default/-files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?;

CENTER FOR COUNTERING DISINFORMATION, *In Sweden nuns were exposed for spying for Russian intelligence*, 19 Januarie 2026, disponibil la https://cpd.gov.ua/en/international-threats-en/europe/in-sweden-nuns-were-exposed-for-spying-for-russian-intelligence/;

CHARLIE DUXBURY, *New Russian church raises suspicions in Swedish town*, Noiembrie 2024, disponibil la https://www.politico.eu/-article/new-russian-orthodox-church-suspicion-sweden-town-vasteras/;

SOROCEANU IGOR, *Dezinformarea în campaniile electorale*, 02 Mai 2025, disponibil la https://revista.universuljuridic.ro/-dezinformarea-in-campaniile-electorale/;

LANCHÈS JULIAN, REKAWEK KACPER, *More of the Same. Russia’s Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited*, 23 Februarie 2026, disponibil https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited;

REKAWEK KACPER, LANCHÈS JULIAN, ZOTOVA MARIA, BOWSER DONALD, *Russia’s Crime–Terror Nexus Criminality as a Tool of Hybrid Warfare in Europe*, Septembrie 2025, disponibil la https://www.globsec.org/sites/default/-

files/202510/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool_0.pdf;

NORDIC DEFENCE REVIEW, *Russian Orthodox Churches in Europe: Espionage Outposts Under the Guise of Faith*, s.a., disponibil la https://nordicdefencereview.com/russian-orthodox-churches-in-europe-espionage-outposts-under-the-guise-of-faith/;

LANGLOIS ROMÉO, NORDSTROM LOUISE, SEIBT SÉBASTIAN, CHABOUR KARINA, France 24, Exclusive investigation: Is the Russian Orthodox Church in Sweden a platform for espionage? disponibil la https://www.france24.com/en/tv-shows/reporters/20250704-exclusive-investigation-is-the-russian-orthodox-church-in-sweden-a-platform-for-espionage.