REZILIENȚA SERVICIILOR DE INTELLIGENCE ÎN ERA RĂZBOIULUI HIBRID

Dr. Răzvan CURCULESCU

Membru al Asociației Resilience Core Initiative-Thor, București

DOI: 10.55535/GMR.2025.3.24

This article provides an exhaustive examination of the operational and institutional resilience of intelligence services in NATO and EU countries in the context of the hybrid war waged by the Russian Federation, as well as the clarification and delimitation of the concept of resilience, as reflected in the programmatic documents of organizations relevant in the field of security, analyzing the measures that can contribute to increasing the resilience of intelligence services, by correlating them to the effects of hybrid warfare on all dimensions of democratic society.

In a period deeply marked by the growth of disinformation, the diversification of cyber-attacks and the increase in the dynamics of influence actions led by state actors, a doctrinal and institutional reset is necessary, as well as the consolidation of cooperation at the level of partner services, through a comparative analysis of public, security policies and strategic documents, highlighting the conceptual and operational differences of NATO and EU states, but also the elements of convergence in the field of resilience from the perspective of designing an integrated intelligence architecture.

Keywords: hybrid warfare; resilience; intelligence services; NATO; EU;

ABORDĂRI CONCEPTUALE – DE LA RĂZBOI HIBRID LA REZILIENȚĂ

Conceptul de *război hibrid*, enunțat și analizat de dr. Frank G. Hoffman în anul 2007, desemna o activitate menită să identifice și să exploateze vulnerabilitățile sistemice ale unui stat considerat țintă, prin acțiuni și operațiuni care nu reprezintă o confruntare directă. În perioada actuală, constatăm că războiul hibrid a devenit parte a confruntării strategice dintre puteri, acesta manifestându-se prin combinarea mijloacelor convenționale și neconvenționale (Hoffman, 2007, p. 8), precum cele cibernetice, informaționale, energetice,economice și nu numai.

Dacă războiul hibrid a fost inițial legat de conflictul din Liban, din 2006, în ultima decadă, se constată că **Federația Rusă** combină mijloace convenționale și neconvenționale, militare și non-militare, într-o campanie coordonată, menită să atingă obiective politice și militare, într-o primă etapă, fără a declara un război deschis. Prin instrumente de tipul: operațiuni cibernetice, campanii de dezinformare, presiuni economice sau energetice, folosirea actorilor *proxy* (miliții, mercenari, organizații criminale), intervenții politice și psihologice, sabotaje, incursiuni cu drone, scopul său este dezbinarea și slăbirea capacității de decizie a adversarului, fără o confruntare clasică (Mumford, 2020, pp. 3-4; Galeotti, 2016, pp. 5-9).

Războiul hibrid exploatează *„ceața informațională" („fog of war")* modernă (Mumford, 2020, p. 5). Actorii hibrizi, statali sau non-statali, lansează simultan fluxuri masive de informații contradictorii (știri false, surse fabricate, date manipulate), menite să satureze capacitatea analitică a adversarului, iar exemplele de mai jos, care expun situații reale, încadrabile în acest tip de război, evidențiază dificultatea contracarării unor astfel de acțiuni.

a. **Eroziunea certitudinii informaționale –** în războiul hibrid dus/purtat de către Federația Rusă, adevărul a devenit un câmp de luptă. Rușii folosesc **dezinformarea, deepfake, manipularea surselor și scurgeri controlate** pentru a polua mediul informațional. Scopul este dublu: **să deturneze analiza internă** a structurilor de *intelligence* din țările vizate și **să submineze încrederea decidenților** în propriul aparat informativ. Astfel, în timpul conflictului din Ucraina (2022-2024), Rusia a lansat simultan narațiuni contradictorii *(„nu există invazie"/„operațiune de eliberare")*, generând confuzie inclusiv în fluxurile OSINT. Serviciile occidentale au contracarat

atacurile ruse pe această dimensiune prin **fuziune multidomeniu și analiză colaborativă NATO-EU-Ucraina** (NATO StratCom COE, 2023).

b. **Creșterea presiunii asupra infrastructurii cibernetice (reziliență tehnologică) –** războiul hibrid include atacuri asupra **infrastructurii IT a serviciilor de *intelligence*** — servere clasificate, canale criptate, baze de date operative sau sisteme SCADA (Supervisory Control and Data Acquisition). Aceste atacuri au scopul de **„a orbi" temporar capacitatea de analiză și reacție**. În 2021, atacurile asupra rețelelor guvernamentale din Ucraina și Polonia (campaniile *„Ghostwriter"* și *„Sandworm"*) au demonstrat cum un adversar poate paraliza temporar comunicarea strategică a serviciilor de *intelligence*. NATO și UE au oferit sprijin comun prin CCDCOE și HybridCoE, testând reacția în regim de criză (ENISA, 2022).

c. **Suprasolicitarea umană și organizațională (reziliență organizațională) –** războiul hibrid impune **activitate continuă, incertitudine permanentă și presiune mediatică**. Serviciile de *intelligence*, obișnuite cu cicluri lineare de informație, trebuie acum să funcționeze într-un regim de alertă constantă. După 2014, serviciile baltice (Estonia, Letonia, Lituania) au introdus programe de formare continuă în *psychological resilience for intelligence analysts*, tocmai pentru a contracara efectele războiului informațional rusesc (HybridCoE, 2021).

d. **Amenințarea credibilității publice (reziliență societală)** – adversarii hibrizi nu atacă doar rețelele informatice, ci și **imaginea publică a instituțiilor de *intelligence***, scopul fiind pierderea încrederii populației și izolarea serviciilor de propriul guvern. În campaniile de dezinformare din Europa Centrală (2018-2022), serviciile au fost ținte directe: acuzații false de spionaj intern sau corupție menite să slăbească încrederea publică. Țările nordice au contracarat prin programe de *strategic communication resilience* coordonate cu NATO StratComCOE (Riga).

e. **Schimbarea paradigmei de apărare (reziliență sistemică)** – războiul hibrid forțează trecerea de la paradigma clasică – *„intelligence reacționează la amenințări"* – la una **proactivă și integrată**: *intelligence previne și modelează mediul de securitate*. Modelul NATO JISR (Joint Intelligence, Surveillance and Reconnaissance) și parteneriatul UE-SIAC sunt exemple concrete de **reziliență sistemică integrată**, care asigură continuitatea informațională chiar și în cazul degradării unui nod de *intelligence* (NATO, 2020; EEAS, 2022).

Plecând de la exemplele menționate, este evident că războiul hibrid obligă serviciile de *intelligence* să devină **organisme vii și adaptive**, capabile să funcționeze în ambiguitate și presiune continuă. Reziliența lor nu mai depinde doar de tehnologie sau secrete, ci de **echilibrul dintre oameni, informație și încredere**. În epoca hibridă, cel mai puternic serviciu de *intelligence* nu este cel care știe cel mai mult, ci cel care **rezistă cel mai bine sub incertitudine** (HybridCoE, 2023, pp. 4-6; Linkov, Kott, 2019, pp. 3-5).

Astfel, putem afirma că războiul hibrid acționează ca un **test de stres permanent** pentru serviciile de *intelligence*, le forțează să își regândească misiunea, structura și cultura internă, în timp ce reziliența nu mai înseamnă doar supraviețuire după un atac, ci și **capacitatea de a funcționa eficient în incertitudine continuă**.

Pe fondul războiului hibrid, serviciile de *intelligence* au devenit principalele instituții care contribuie la consolidarea rezilienței statelor țintă, piloni în reziliența strategică, prin îndeplinirea misiunilor de avertizare timpurie și protejare a deciziei.

Conceptual, vom defini *reziliența* ca fiind capacitatea unui sistem de a absorbi șocuri și de a-și menține funcțiile esențiale în situații de criză. Adaptând conceptul la subiectul prezentei cercetări, putem considera că reziliența serviciilor de *intelligence* reprezintă starea în care acestea sunt adaptate operațional, organizațional și cognitiv pentru a face față situațiilor de criză, generate de războiul hibrid.

În literatura de specialitate regăsim conceptul de reziliență tratat din diferite perspective – *reziliență societală* (Chandler, 2014, p. 56), *reziliență tehnologică* (Linkov, Trump, 2019, pp. 9-34), dar cel de *reziliență statală*, strategică sau, punctual, al serviciilor de *intelligence* este un domeniu în care acest concept este relativ nou. Un punct important în definirea acestuia îl reprezintă momentul anexării ilegale a Peninsulei Crimeea de către Federația Rusă (2014), care a determinat NATO și UE să conceptualizeze noțiunea de reziliență la nivelul celor două organizații internaționale.

În anul 2022, NATO (NATO, 2022) și, ulterior, UE, în 2023 (ENISA, 2023), au lansat o serie de politici menite a consolida reziliența statelor față de amenințările războiului hibrid, fiind subliniate amenințările cibernetice și agresiunile informaționale ca factori de risc ridicat în afectarea securității statelor membre. În acel context, putem constata statuarea principiului că reziliența serviciilor de *intelligence* era direct influențată de adaptarea capacităților operaționale la acest nou tip de amenințări. Reținem aici cadrul de referință statuat de către NATO prin definirea celor *„șapte cerințe de bază pentru reziliență”* (NATO, 2016,

para. 73), dar și mecanismele instituite de UE prin *Hybrid Fusion Cell* (European Commission&High Representative, 2016, Hybrid Fusion Cell Section) și *Strategia de Securitate Cibernetică* (European Commission, 2020).

Analiza comparativă a modului în care cele două organizații abordează conceptul de reziliență va evidenția elementele de divergență și convergență, dar va sublinia faptul că reziliența serviciilor occidentale de *intelligence* nu va fi realizabilă în absența unei cooperări profunde.

Studiul datelor din spațiul public relevă faptul că termenul de reziliență are o semnificație complexă. Pornind de la abordarea teoretică care arată că un sistem, oricare ar fi acela, este rezilient dacă are capacitatea de a-și menține funcțiile de bază în cazul unor crize, particularizând, observăm că, în cazul serviciilor de *intelligence,* aceste crize, pe care le putem denumi și *perturbări*, pot fi legate de terorism, spionaj, atacuri cibernetice, crize energetice și chiar economice.

Observăm că, în domeniul securității, și, în mod special, al zonei de *intelligence*, conceptul de reziliență va include ca principali actori statele, cu toate componentele lor ce necesită a fi apărate, indiferent de tipul amenințărilor generate de războiul hibrid. Altfel spus, reziliența serviciilor de *intelligence* devine un garant al capacității statelor de a gestiona amenințările și a-și recupera funcționalitățile de bază în cazul unor incidente de securitate. În acest fel, statele vor reuși menținerea stabilității sociale și politice, necesare dezvoltării economice și menținerii statului de drept.

Pe acest fond, reziliența serviciilor de *intelligence* va fi dată de capacitatea acestora de a anticipa amenințările și de a adapta măsuri proporționale cu scopul protejării valorilor democratice, a infrastructurilor critice și a politicilor publice. Anticiparea reprezintă una dintre cele mai dificile și complexe misiuni în zona de *intelligence* (Lowenthal, 2017, p. 148) și nu poate fi realizată în absența unei creșteri a capacității de obținere de informații, inclusiv prin cooperare, dar mai ales prin creșterea capacității de analiză strategică a acestora. Experiența a arătat că adaptarea serviciilor de *intelligence* este dată, în primul rând, de capacitatea acestor structuri de a învăța rapid și eficient din activitatea proprie, dar și din experiența partenerilor.

Așadar, pornind de la interpretarea generală a rezilienței, putem considera că reziliența unui serviciu de *intelligence* reprezintă capacitatea de a anticipa, gestiona, contracara și reveni după o criză *(perturbare)*. Pentru susținerea argumentației, prin *perturbare* se va înțelege orice acțiune directă sau indirectă, ce nu a fost anticipată, precum: scurgeri de informații, atacuri cibernetice, presiuni politice, manipulare informațională sau disfuncție majoră (economică, politică, socială, militară).

Pe baza acestor abordări conceptuale, în contextul amenințărilor specifice războiului hibrid, se pot detalia elementele caracteristice ale rezilienței serviciilor de *intelligence* din spațiul euroatlantic, prin gruparea lor pe dimensiuni, astfel:

❖ Reziliența **organizațională** (Lengnick-Hall, Beck, Lengnick-Hall, 2011, p. 244), ca fiind maniera în care serviciile de *intelligence* reușesc, prin practicarea unui management modern și o cultură organizațională bazată pe *leadership*, să adapteze rapid organizația la schimbările în plan operațional care pot provoca perturbări în activitatea specifică. Adaptarea organizațională optimă la schimbările tehnologice și geopolitice generate de războiul hibrid va constitui un factor cheie în păstrarea încrederii și menținerea moralului celor care activează în acest domeniu, pentru îndeplinirea misiunilor serviciilor din care aceștia fac parte.

❖ Reziliența **informațională** (Wardle, Derakhshan, 2017, p. 16) este reprezentată de creșterea calității informațiilor obținute și de capacitatea superioară de analiză și integrare a acestora pentru a putea cunoaște și contracara atacurile la adresa serviciilor de *intelligence*. În general, atacurile pot fi de tipul *fakenews* sau dezinformări cu privire la rolul și locul unui serviciu într-un stat democratic. Deși foarte rar în spațiul euroatlantic, au existat situații în care anumite persoane au trădat interesele unor servicii și, implicit, ale statelor de origine. Pe acest fond, reziliența informațională va fi realizată în situația în care serviciile de *intelligence* vor adapta regulile interne astfel încât să fie prevenite eventualele infiltrări, scurgeri de informații, surse duble sau chiar defectări.

Dacă cele două dimensiuni țin foarte mult de capacitatea intrinsecă a serviciilor de *intelligence* de a fi reziliente și, de cele mai multe ori, aspectele enumerate sunt mai puțin cunoscute publicului larg, următoarele dimensiuni ale rezilienței serviciilor de informații sunt, de regulă, vizibile și de natură a afecta grav securitatea statelor din care fac parte și, implicit, a securității spațiului euroatlantic.

❖ Reziliența **operațională** (Duchek, 2020, p. 215) a serviciilor de *intelligence* este dată de capacitatea permanentă de a obține, analiza și valorifica informații strategice chiar și atunci când există situații de criză. Războiul hibrid va genera permanent situații noi, uneori neanticipate, prin valorificarea noilor tehnologii inovative, concomitent cu exploatarea vulnerabilităților. Avem în vedere aici un posibil atac cibernetic sau un act de sabotaj asupra infrastructurilor critice.

❖ Reziliența **societală** se referă la capacitatea unei societăți de a absorbi șocuri majore (dezastre naturale, pandemii, crize economice etc.), de a se adapta și de a-și reveni după șoc (Chandler, 2014, p. 56), astfel că vom avea în vedere că, într-un stat

democratic, un serviciu de *intelligence* va avea un loc important în dimensiunea societală, ca parte integrantă a societății, cu un rol bine definit de apărare a populației, a deciziilor strategice, a infrastructurilor critice față de noile provocări generate de războiul hibrid.

❖ Reziliența **strategică** (Hamel, Välikangas, 2003, p. 52) este, în opinia mea, cea mai importantă dimensiune a unui serviciu de *intelligence* în situația apariției unor factori perturbatori majori precum cei specifici războiului hibrid. Rolul unui serviciu de *intelligence* în menținerea capacității decizionale a unui stat în momente de criză majoră (război sau afectarea severă a infrastructurii critice) este esențial într-un stat democratic.

REZILIENȚA SERVICIILOR DE *INTELLIGENCE* ÎN STRUCTURILE EUROATLANTICE

Pentru a înțelege mai bine domeniul, vom face o analiză comparativă a modului în care este abordată reziliența la nivelul NATO și al UE, prezentând, totodată, și o serie de considerente referitoare la modul în care România abordează acest domeniu.

Organizația Tratatului Atlanticului de Nord/NATO este **o alianță politico-militară**, formată în 1949 cu scopul principal de a asigura **apărarea colectivă** a statelor membre. NATO este *„o alianță politică şi militară a ţărilor din Europa şi America de Nord, al cărei scop este să garanteze libertatea şi securitatea membrilor săi prin mijloace politice şi militare.”* (NATO, What is NATO?).

Uniunea Europeană/UE este **o uniune politică și economică** formată din **27 de state europene** care au decis să coopereze strâns pentru a asigura pacea, stabilitatea și prosperitatea pe continent. Rolul principal al UE este acela de a facilita cooperarea între statele membre, astfel încât acestea să fie **mai puternice împreună decât separat**, menținând pacea și susținând dezvoltarea economică și socială (EU, What is the European Union?).

Având în vedere înseși definițiile celor două organizații, se poate deduce că și reziliența este abordată pe specificul fiecărei organizații, însă politicile și strategiile adoptate converg către același obiectiv, și anume creșterea rezilienței. Ambele organizații, NATO și UE, au dezvoltat un mix de politici și strategii prin care se construiește reziliența serviciilor de *intelligence*, dar și structuri comune dedicate analizei integrate, derularea unor exerciții comune și îmbunătățirea cadrului legislativ necesar consolidării cooperării. Astfel, putem afirma că un efect

al amenințărilor războiului hibrid este inclusiv întărirea cooperării politico-militare cu societatea civilă pentru creșterea rezilienței societale, în special la atacurile cibernetice și dezinformare.

REZILIENȚA SERVICIILOR DE *INTELLIGENCE* ÎN NATO

Din studierea documentelor (NATO, Resilience Committee, 2022) de planificare și conducere ale organizației se constată că NATO consideră **reziliența ca fiind elementul cheie** în politica sa de descurajare a amenințărilor războiului hibrid, prin solicitarea permanentă către aliați de a întreprinde permanent măsuri necesare asigurării capacităților operaționale în situații de criză. Conform NATO, *„capacitatea naţională şi colectivă de reziliență reprezintă o bază esenţială pentru credibilitatea descurajării."* (NATO, 2024).

NATO a inițiat, susținut și dezvoltat conceptul de capacități comune de prevenire și a sprijinit constituirea unor **structuri de analiză integrată**, precum *Joint Intelligence and SecurityDivision* (JISR) și *NATO Intelligence Fusion Centre* (NIFC) (NATO, 2024). În concret, activitatea acestor structuri a sporit schimbul de informații între aliați și, în consecință, a contribuit la creșterea calității deciziilor în plan operațional. De exemplu, NIFC *„furnizează SACEUR (Supreme Allied Commander Europe) informaţii relevante, exacte şi la timp pentru a sprijini planificarea şi executarea operaţiunilor"* (NATO Intelligence Fusion Centre, *„Mission"* section).

În domeniul apărării cibernetice, NATO a demarat o serie de **exerciții comune** prin care statele partenere își pot antrena specialiștii prin participarea în astfel de formate. Spre exemplu, prin centrul *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) din Tallinn, NATO creează scenarii realiste de apărare prin care crește reziliența serviciilor de *intelligence* în contextul în care acestea au devenit tot mai dependente de infrastructurile digitale. Prin aceste exerciții comune, serviciile de *intelligence* au dezvoltat capacitatea de interoperabilitate și de răspuns adecvat la amenințările specifice războiului hibrid.

În esență, doctrina NATO în domeniul apărării consideră că reziliența militară include *„pregătirea civilă şi comercială de care forţa militară are nevoie pentru a desfăşura trupe rapid şi liber în întreg teritoriul Alianţei"* (NATO, 2022, secțiunea despre *„layered resilience"*).

Un ultim aspect pe care îl avem în vedere în analizarea creșterii rezilienței serviciilor de *intelligence* este faptul că NATO a urmărit și a reușit **standardizarea unitară a comunicării** la nivelul Alianței.

Astfel, prin instrumente de tip ***Joint Intelligence, Surveillance and Reconnaissance*** (JISR) – *cadru integrat în domeniul militar prin care se combină*

capabilităţile de informaţii (Intelligence), supraveghere (Surveillance) şi recunoaştere (Reconnaissance), pentru a sprijini deciziile strategice şi operaţionale și ***Federated Mission Networking*** (FMN) – *care este o inițiativă a NATO care are drept scop crearea rapidă şi interoperabilă a reţelelor de misiune („mission networks") pentru forţele aliate şi partenere într-operaţiuni comune,* NATO a redus riscul apariției unor *„single points of failure"* în operațiunile comune.

Ca o concluzie a modului în care reziliența contribuie la apărarea colectivă, menționăm *Doctrina Allied Joint* din cadrul publicației *Allied Joint Publication* (AJP) care subliniază că *„formarea puterii combinate … necesită reziliență stratificată în contextul apărării"* (NATO, 2022, p. 73).

REZILIENȚA SERVICIILOR DE *INTELLIGENCE* ALE STATELOR MEMBRE ALE UE

În contextul intensificării amenințărilor hibride generate de acțiunile Federației Ruse, în special cibernetice, dar și al unui mediu de securitate cu o dinamică rapidă a evoluției și, implicit, o schimbare a mediului strategic, UE a adoptat o serie de instrumente politice şi normative cu scopul consolidării rezilienţei sale strategice cu impact direct în consolidarea rezilienței serviciilor de *intelligence*.

Pentru a oferi o mai mare claritate pe acest subiect, în acest articol vom trece în revistă elementele cheie ale măsurilor UE care contribuie la reziliența strategică și operațională a serviciilor de *intelligence* din statele membre ale UE, astfel: Strategic Compass şi Single Intelligence Analysis Capacity (SIAC); instrumentele împotriva amenințărilor hibride; reglementările şi standardele cibernetice; cooperarea practică şi capabilităţile comune.

a. **Strategic Compass&SIAC (Single Intelligence Analysis Capacity)** – *Strategic Compass* este documentul de orientare strategică al UE în domeniul securității și apărării, adoptat de către Consiliul Uniunii Europene în martie 2022, prin care au fost stabilite obiective concrete până în 2030, pentru consolidarea rezilienței, prin măsuri de creștere a capacităților europene de anticipare, evaluare a riscurilor și gestionare a crizelor. Busola strategică este construită pe patru piloni *(„Act", „Invest", „Partner" şi „Secure")* şi include măsuri pentru anticiparea, descurajarea şi răspunsul la ameninţări (Consilul UE, 2022).

În acest context, SIAC, care are în componență EU INTCEN (componenta civilă de *intelligence*) și EUMS-INT (componenta militară din cadrul Statului Major al UE), a fost conceput ca un punct unic pentru analiză strategică integrată, cu un rol central în furnizarea de cunoaștere (Blockmans, Crosson, Paikin, 2022, pp. 4-6).

Structurarea sa ca un *„single entrypoint”* pentru analiză strategică furnizată de statele membre a permis integrarea fluxurilor de informații civile și militare cu scopul creșterii calității produselor analitice comune. Prin introducerea acestui mecanism s-a constatat o creștere a coerenței deciziilor strategice la nivelul decidenților UE și o imagine de ansamblu mai clară a amenințărilor războiului hibrid. Pe acest fond, UE și-a consolidat reziliența strategică pentru gestionarea crizelor complexe.

b. **Reglementări și standarde cibernetice**: NIS2 și rolul ENISA (European Union Agency for Cybersecurity) – noua directivă NIS2 (Network and Information Security Directive) este cadrul legal-fundamental al UE pentru asigurarea unui nivel înalt comun de securitate cibernetică în sectoare esenţiale. Reprezintă cel mai amplu cadru legislativ european pentru protejarea infrastructurilor critice și extinde cerințele de securitate la mai multe sectoare – energie, transport, sănătate, administrație publică, telecomunicații, finanțe, furnizori de servicii digitale etc. (UE, Directivă 2022/2555).

Principalele efecte ale NIS2 asupra rezilienței includ: obligații clare de prevenire, detectare și raportare rapidă a incidentelor cibernetice; cerințe de guvernanță și management al riscului la nivelul conducerii organizațiilor; standarde minime privind securitatea rețelelor și a lanțurilor de aprovizionare; sancțiuni mai severe pentru neconformitate. Astfel, prin această Directivă au fost introduse elemente stricte privind managementul riscului, raportarea incidentelor şi cooperarea transfrontalieră.

Agenţia ENISA are rol central în cunoașterea și implementarea directivelor din domeniul cibernetic. Cu un rol extins în implementarea actelor legislative obligatorii ale Uniunii Europene, ENISA oferă: ghiduri tehnice și bune practici, coordonarea răspunsurilor între statele membre, evaluări ale amenințărilor (Threat Landscape Reports), sprijin pentru testarea și auditarea infrastructurilor critice. (UE, 2019, art. 8-11).

Împreună, NIS2 și ENISA ridică nivelul general de **cyberhygiene**, reduc vulnerabilitățile structurale și îngustează suprafața de atac exploatabilă de către adversari – aspect esențial pentru reziliența serviciilor de *intelligence*, a infrastructurilor lor digitale, a infrastructurilor critice și, în concluzie, a statelor membre (UE-ENISA, 2023, pp. 6-7).

c. **Instrumente împotriva amenințărilor hibride**. Prin cooperarea cu NATO, UE a creat *Centrul European de Excelență pentru Combaterea Amenințărilor Hibride* (HybridCoE), acesta fiind principala platformă de cooperare în gestionarea în comun a amenințărilor hibride (European Commission&High

Representative, 2016, *Hybrid Threats Section*). Centrul funcționează ca un *hub* de expertiză pentru identificarea, analiza și reacțiile la amenințările hibride, în domenii precum: campanii de dezinformare și manipulare, interferență politică străină, război informațional, presiuni economice și energetice, combinația dintre operațiuni cibernetice și acțiuni fizice (sabotaj, provocări la frontieră etc.).

HybridCoE nu doar produce analize și scenarii complexe, ci organizează și exerciții multilaterale, instruire aplicată și proiecte comune. În acest fel, centrul consolidează **reziliența societală** și capacitatea sectorială de reacție, în următoarele direcții:

- crește capacitatea instituțiilor de a recunoaște și contracara interferențele;
- oferă instrumente pentru răspuns coordonat între sectoare (guvern, infrastructuri, mediul privat);
- contribuie la sincronizarea măsurilor între UE, NATO și statele participante.

d. Cooperare practică și capabilități comune. Pe lângă cadrele instituţionale şi normative, UE a investit și în instrumente operaţionale care contribuie la interoperabilitatea între serviciile de *intelligence*. Aceste instrumente au un rol major în creșterea rezilienței acestor servicii în gestionarea amenințărilor hibride ale Federației Ruse. Pe această dimensiune, sunt relevante următoarele elemente:

- **Capabilități spațiale și satelitare** (ex. Galileo, Copernicus), care asigură comunicații sigure, imagistică avansată și monitorizarea mediilor critice.
- **Centre de imagistică și analiză geospațială**, care sprijină **Politica de Securitate și Apărare Comună (PSAC)** și răspunsul la crize.
- **Inițiativa Permanent Structured Cooperation (PESCO)**, menită să creeze capabilități comune (ex. comandamente medicale la supraveghere maritimă, rețele de comunicații securizate).
- **Proiecte din cadrul PSAC,** care includ instruire comună, partajare de informații și dezvoltarea de instrumente pentru gestionarea crizelor.

În concluzie, prin cele menționate, UE a reușit sa proiecteze o arhitectură menită a consolida reziliența statelor și, implicit, a serviciilor de *intelligence*, aceste mecanisme fiind de natură a consolida reziliența UE, în ansamblul său, prin crearea unui mediu de securitate integrat, capabil să genereze reacții adecvate la amenințările în continuă evoluție generate de către Federația Rusă.

OPȚIUNILE ROMÂNIEI CA MEMBRU AL NATO ȘI AL UE

Începând cu anul 2014, în contextul anexării ilegale a Peninsulei Crimeea, România a inițiat un amplu proces de **aliniere doctrinară** la standardele NATO și ale UE, reflectat în *Strategia Națională de Apărare a Țării (2020-2024)* și în reformele interne ale serviciilor de informații. Plecând de la acestea, **reziliența națională** poate fi înțeleasă drept **capacitatea instituțiilor statului, a economiei și a societății de a proteja funcțiile esențiale, de a preveni și a gestiona perturbările majore și de a reveni rapid la starea de normalitate**, în concordanță cu abordarea de *„securitate națională extinsă"* definită în Strategia Națională de Apărare a Țării (Administrația Prezidențială, 2020, pp. 7-8).

Pe lângă aceste linii directoare, sunt indicate și instituțiile-cheie implicate în implementarea politicilor de securitate, *intelligence* și reziliență în România:

❖ **Serviciul Român de Informații (SRI)** este principalul serviciu de informații interne al României și acționează ca *autoritate națională* în domeniul securității cibernetice. În acest rol, SRI coordonează politicile de **reziliență cibernetică**, gestionează protecția infrastructurilor critice de interes național și asigură prevenirea, detectarea și contracararea amenințărilor cibernetice și teroriste. Prin Centrul Național Cyberint și prin cooperarea cu Direcția Națională de Securitate Cibernetică/DNSC, SRI contribuie la întărirea capacităților naționale de răspuns la incidente și contracarează atacuri cibernetice complexe (Ib., pp. 26-27, 34).

❖ **Serviciul de Informații Externe (SIE)** are responsabilitatea de a colecta, analiza și furniza decidenților informații privind **riscurile și amenințările externe** la adresa României. În contextul rezilienței naționale, SIE monitorizează evoluțiile geopolitice, crizele internaționale, riscurile hibride, atacurile cibernetice provenite din afara țării, precum și actorii ostili. De asemenea, SIE coordonează cooperarea internațională cu servicii partenere, organizații precum NATO și UE și facilitează schimbul de informații strategice relevante pentru securitatea națională, serviciul fiind responsabil de evaluarea riscurilor externe și cooperarea internațională. Pe fondul războiului hibrid, SIE a intensificat cooperarea cu structurile UE, participând la fluxurile analitice ale **INTCEN** și ale **Hybrid Fusion Cell** (Serviciul de Informații Externe, n.d., Misiune și cooperare internațională).

❖ **Consiliul Suprem de Apărare a Țării (CSAT)** reprezintă **nivelul strategic de integrare** a politicilor de securitate, apărare și *intelligence*. Consiliul aprobă strategiile naționale (ex.: Strategia Națională de Apărare a Țării, Strategia de Securitate Cibernetică etc.), stabilește prioritățile în domeniul informativ-operativ,

coordonează activitatea instituțiilor de *intelligence* și validează măsurile necesare pentru consolidarea rezilienței naționale. CSAT funcționează ca platformă unificată de decizie între Președintele României, Guvern și structurile cu responsabilități în domeniu, funcționând ca un integrator strategic al politicilor de *intelligence* și reziliență.

România a început să dezvolte, după 2020, o **componentă de reziliență cognitivă**, axată pe educația strategică și pe combaterea dezinformării. Campanii precum *#SiguranțaOnline* (DNSC, 2022) și programele universitare de *cyberdiplomacy* și *analiză strategică* contribuie la formarea unei *„culturi a rezilienței"* în spațiul public.

În cooperare cu StratCom COE, România a implementat exerciții de comunicare strategică și simulări de gestionare a crizelor informaționale, inclusiv scenarii de dezinformare în timpul alegerilor. Această dimensiune societală completează arhitectura de reziliență tehnologică, aducând în prim-plan ideea de **securitate cognitivă** – apărarea capacității colective de a distinge adevărul de manipulare (Waltzman, 2017, p. 2).

Deși România a înregistrat progrese semnificative, în opinia mea, persistă totuși o serie de vulnerabilități structurale, precum: fragmentarea instituțională dintre SRI, SIE și alte agenții guvernamentale; deficitul de personal specializat în analiza datelor și *intelligence* digital; dependența tehnologică de furnizori externi în infrastructura IT guvernamentală; legislația încă rigidă privind schimbul de date între instituții. Totuși, aceste provocări sunt parțial compensate prin cooperarea internațională și prin procesul continuu de învățare instituțională.

Analiza comparativă a modului în care România abordează conceptul de reziliență în raport cu NATO și cu UE a evidențiat faptul că țara noastră se poziționează într-o zonă de **convergență doctrinară** între cele două organizații euroatlantice. Această poziționare strategică nu este doar o consecință a apartenenței duble, ci rezultatul unei **politici deliberate de adaptare instituțională**. În opinia mea, în ultimii zece ani, serviciile de *intelligence* din România au trecut de la o paradigmă defensivă, centrată pe protecția informației, la una proactivă, bazată pe **anticipare, partajare și adaptabilitate**.

Prin cooperarea constantă cu **centrele de excelență NATO (CCDCOE, StratCom COE)** și prin participarea la mecanismele europene de analiză (INTCEN, Hybrid Fusion Cell), România a dezvoltat o **reziliență multiplă**, care combină capabilitățile militare, civile și cognitive, astfel că România este descrisă în literatura de specialitate ca un *„hub emergent de securitate cibernetică"* în Europa de Est (Popescu, 2022).

Totuși, această poziționare aduce și vulnerabilități, mai ales că proximitatea geografică față de spațiile conflictuale (Marea Neagră, Ucraina, Republica Moldova) amplifică presiunea asupra structurilor de *intelligence* din țara noastră.

În domeniul *intelligence*, **reziliența cognitivă** se referă la capacitatea analiștilor și decidenților de a recunoaște, interpreta și reacționa la informațiile manipulative. Aceasta este strâns legată de **reziliența instituțională**, care presupune structuri flexibile și fluxuri informaționale rapide. Din necesitatea de a face față cât mai eficient actualelor provocări cu care se confruntă, România a început să integreze aceste două niveluri prin programe de formare interdisciplinară, precum:

- cursurile de *intelligence strategic și analiza decizională,* organizate la Academia Națională de Informații *„Mihai Viteazul”*;
- cooperarea SRI-MAE-DNSC pentru instruirea personalului din domeniul *cyberdiplomacy*;
- parteneriatele cu universități civile pentru cercetarea dezinformării (Universitatea București, SNSPA, Universitatea Babeș-Bolyai).

Această abordare, în care procesul de analiză este dublat de un mecanism intern de autocorecție și învățare instituțională, inspirată din teoria sistemelor complexe (Chandler, 2014), oferă flexibilitate în gestionarea incertitudinii și reduce riscul de erori cognitive în procesul decizional strategic.

În concluzie, având în vedere cele expuse mai sus, la nivel teoretic, România asimilează modelele de creștere a rezilienței serviciilor de *intelligence* din spațiul euroatlantic, unde NATO oferă cadrul strategic de apărare și UE furnizează arhitectura de guvernanță și cooperare civilă. În ansamblu, serviciile de *intelligence* din România **evoluează de la o securitate reactivă la reziliență**, având o bază solidă în capacitatea de a învăța și de a se adapta la contextul securitar generat de războiul hibrid condus de către Federația Rusă (Manea, 2021, pp. 52-53).

CONCLUZII

Analiza desfășurată în acest articol științific confirmă faptul că **reziliența serviciilor de *intelligence*** reprezintă o componentă esențială a arhitecturii de securitate a secolului XXI, în special în contextul războiului hibrid.

În esență, **NATO** se concentrează pe interoperabilitate, capacități militare comune și exerciții colective, în timp ce **UE** promovează coordonare strategică, reglementare cibernetică și reziliență societală. NATO și UE, deși pornesc de la paradigme instituționale distincte, converg către o **viziune comună:** protejarea societăților democratice printr-un sistem de *intelligence* capabil să anticipeze, să absoarbă și să se adapteze la șocuri complexe. Una dintre cele mai sensibile

probleme ale rezilienței în *intelligence* este **echilibrul dintre transparență și securitate**, astfel că, în timp ce UE promovează o cultură a guvernanței deschise, NATO și structurile naționale de *intelligence* operează tradițional într-un cadru restrâns, de confidențialitate.

În măsura în care vor fi depășite elemente de tipul încredere versus partajare (uneori, anumite rivalități limitează schimbul de informații); limitări legale/ constituționale (date de suveranitatea statelor); dependența de unele infrastructuri private (care, uneori, nu respectă aceleași standarde de secretizare/securitate), reziliența serviciilor de *intelligence* va atinge un nivel optim pentru contracararea amenințărilor hibride care devin din ce în ce mai complexe, prin îmbinarea a multiple tipuri de manifestări (ex: combinare atac cibernetic cu dezinformare).

România, aflată la intersecția acestor două sisteme, reușește în domeniul serviciilor de *intelligence* să-și construiască o **reziliență mixtă**, adaptată propriilor nevoi și vulnerabilități. Prin reformarea în raport cu standardele NATO și ale UE, serviciile de *intelligence* din România au devenit parte activă a fluxurilor de informații, au dovedit că au capacitatea de a se adapta instituțional și de a dezvolta capacități de analiză strategică și, implicit, reziliență operațională adecvată pentru gestionarea amenințărilor războiului hibrid dus de către Federația Rusă împotriva spațiului euroatlantic.

BIBLIOGRAFIE:

1. Administrația Prezidențială (2020). *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. O Românie sigură și prosperă într-o lume marcată de noi provocări*, București, https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020.pdf, accesat la 15 octombrie 2025.
2. Blockmans S., Crosson D.M., Paikin Z. (2022). CEPS Policy Insights, https://cdn.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-14_EU-Strategic-Compass.pdf, accesat la 14 octombrie 2025.
3. Chandler, D. (2014). *Resilience: The Governance of Complexity*. Routledge.
4. Council of the European Union (2022). *A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security*, https://www.consilium.europa.eu/en/policies/strategic-compass/, accesat la 12 octombrie 2025.
5. Duchek, S. (2020). *Organizational resilience: A capability-based conceptualization*, Business Research, 13(1), pp. 215-246.
6. ENISA (2023). *ENISA Work Programme 2023*. European Union Agency for Cybersecurity. European Union, https://www.enisa.europa.eu/publications/corporate-documents/work-programme-2023, accesat la 12 octombrie 2025.

7. ENISA (26 iunie 2025). *NIS2 technical implementation guidance*. European Union Agency for Cybersecurity, https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance, accesat la 10 octombrie 2025.
8. European Commission&High Representative of the Union for Foreign Affairs and Security Policy (2016). Joint framework on countering hybrid threats: A European Union response, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018, accesat la 11 octombrie 2025.
9. European Commission (2020). *The EU's cybersecurity strategy for the digital decade*, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade, accesat la 11 septembrie 2025.
10. European External Action Service (EEAS) (2022). *EU Single Intelligence Analysis Capacity (SIAC): Overview and functions*, Brussels: EEAS, https://www.eeas.europa.eu, accesat la 11 octombrie 2025.
11. European External Action Service (2022). EU Intelligence and Situation Centre (INTCEN): Overview and functions, https://www.eeas.europa.eu, accesat la 10 octombrie 2025.
12. European Union Agency for Cybersecurity (ENISA) (31 ianuarie 2023). *The NIS2 Directive: Network and information systems directive 2*, https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2, accesat la 10 octombrie 2025.
13. European Union. *What is the European Union?*, https://op.europa.eu/webpub/com/eu-and-me/en/WHAT_IS_THE_EUROPEAN_UNION.htm, accesat la 10 octombrie 2025).
14. Galeotti, M. (2016). *Hybrid War or Gibridnaya Voyna?,* Getting Russia's non-linear military challenge right. Mayak Intelligence Report.
15. Hamel, G., Välikangas, L. (2003). *The quest for resilience*, în *Harvard Business Review*, 81(9), pp. 52-65
16. Hoffman, F.G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.
17. Hybrid Centre of Excellence (2021). *Building resilience against hybrid threats: Lessons learned from the Baltic region*. Helsinki: HybridCoE.
18. Hybrid Centre of Excellence (2023). Hybrid influence operations and resilience. Helsinki: HybridCoE.
19. Lengnick-Hall, C.A., Beck, T.E., Lengnick-Hall, M.L. (2011). *Developing a capacity for organizational resilience through strategic human resource management*, în *Human Resource Management Review*, 21(3), https://doi.org/10.1016/j.hrmr.2010.07.001, accesat la 21 septembrie 2025.
20. Linkov, I., Kott, A. (2019). *Fundamentals of cyber resilience: Building a secure and resilient digital society*. Springer.
21. Linkov, I., Trump, B.D. (2019). *The science and practice of resilience*. Springer.
22. Lowenthal, M.M. (2017). *Intelligence: From secrets to policy* (7th ed.). CQ Press.
23. Manea, A. (2021). *Adaptabilitatea serviciilor de informații românești în contextul amenințărilor hibride*. Analize de Securitate, 10(2), pp. 45-63.

24. Mumford, A. (2020). *Ambiguity in hybrid warfare*. Helsinki. The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf, accesat la 15 octombrie 2025.
25. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2021). Locked Shields 2021 after-action report. Tallinn: CCDCOE, accesat la 15 octombrie 2025.
26. NATO Intelligence Fusion Centre (n.d.). *Who we are/Mission*, https://web.ifc.bices.org.html, accesat la 12 octombrie 2025.
27. NATO StratCom Centre of Excellence (2023). *Resilience in the information environment: Countering hybrid narratives.* Riga: NATO StratCom COE, accesat la 12 octombrie 2025.
28. NATO, https://ccdcoe.org/locked-shields, accesat la 11 octombrie 2025.
29. NATO, https://www.act.nato.int/activities/federated-mission-networking.html, accesat la 11 octombrie 2025.
30. NATO, https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf, accesat la 11 octombrie 2025.
31. NATO, https://www.nato.int/en/about-us/organization/nato-structure/resilience-committee, 7 octombrie 2022, accesat la 11 octombrie 2025)
32. NATO (2016). *Commitment to enhance resilience* (Warsaw Summit Communiqué, para. 73). North Atlantic Treaty Organization, https://www.nato.int, accesat la 11 octombrie 2025.
33. NATO (2020). *Joint Intelligence, Surveillance and Reconnaissance* (JISR). Brussels: NATO Public Diplomacy Division, https://www.nato.int/en/what-we-do/deterrence-and-defence/joint-intelligence-surveillance-and-reconnaissance, accesat la 11 octombrie 2025.
34. NATO (2022), https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf, accesat la 12 octombrie 2025.
35. NATO (2022). *Resilience and defence: Strengthening NATO's deterrence and defence posture.* Brussels: NATO.
36. NATO (2024). *Resilience, civil preparedness and Article* 3, https://www.nato.int/cps/en/natohq/topics_132722.htm, accesat la 10 octombrie 2025.
37. North Atlantic Treaty Organization. What is NATO?, https://www.nato.int/en/what-is-nato.html, accesat la 10 octombrie 2025.
38. Popescu, A. (2022). *Evoluții recente în securitatea cibernetică din Europa Centrală și de Es*t, în Revista Română de Studii de Securitate, 5(2), pp. 45-60.
39. Rathje, S., Navarre, A. (2022). *What Is Societal Resilience?* AXA Research Fund.
40. Serviciul de Informații Externe (n.d.). *Misiune și cooperare internațională*, https://www.sie.ro/, accesat la 12 octombrie 2025.
41. Serviciul Român de Informații (2023). *Raport de activitate 2022-2023*. București.
42. UE (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act), în Official Journal of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881, accesat la 12 octombrie 2025.

43. Waltzman, R. (2017). *The weaponization of information: The need for cognitive security* (Testimony before the U.S. Senate Armed Services Committee). RAND Corporation, https://www.rand.org/pubs/testimonies/CT473.html, accesat la 12 octombrie 2025.
44. Wardle, C., Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy maki*ng (p. 16). Council of Europe.