

NOTĂ DE ANALIZĂ STRATEGICĂ

Privind implementarea programului SAFE

Programul SAFE oferă României o oportunitate istorică de a accelera modernizarea capacităților de apărare și de a consolida integrarea în ecosistemul european și euro-atlantic de securitate. Totuși, analiza empirică a programelor majore de înzestrare demonstrează că riscurile critice apar rareori în etapa strict contractuală sau de achiziție de tehnologie (**Output**). Acestea se manifestă sistemic în fazele de implementare, integrare operațională și susținere pe termen lung (**Outcome**).

Prezenta notă identifică și evaluează factorii de risc structurali grupați pe modelul doctrinar NATO (**DOTMLPFI**). Concluzia fundamentală indică faptul că succesul programului SAFE va depinde direct de capacitatea instituțională a statului de a integra simultan resursa umană, doctrinele tactice și infrastructura logistică.

În termeni militari s-ar numi operaționalizare. Fără o mutare a accentului decizional de la procesul de achiziție la cel de transformare instituțională, investițiile masive riscă să producă doar o modernizare fragmentată, lipsită de relevanță operațională reală în caz de criză.

1. Context Strategic și Premise Doctrinare

Semnarea contractelor și recepția fizică a echipamentelor reprezintă doar faza incipientă a ciclului de viață al unei capacități militare. Experiența recentă a statelor membre NATO demonstrează că performanța unei forțe este determinată de echilibrul perfect între trei componente interdependente:

1.1 Tehnologia (Platforma hardware/software): Vectorul tehnic propriu-zis.

1.2 Resursa Umană: Gradul de instruire, specializare și retenție a personalului.

1.3 Procesele Organizaționale: Doctrinele de angajare în luptă, structurile de comandă-control și flexibilitatea fluxurilor decizionale.

Orice dezechilibru sau asimetrie în ritmul de dezvoltare a acestor componente generează vulnerabilități operaționale severe și reduce dramatic randamentul investițiilor de capital. Din acest motiv, implementarea programelor SAFE trebuie abordată la cel mai înalt nivel decizional ca un efort de **transformare instituțională extinsă**, depășind paradigma clasică a managementului de achiziții publice.

2. Matricea Principalelor Riscuri Structurale

Nr. Crt.	Categoria de Risc	Indicator Specific	Probabilitate Impact	Nivel Risc	Proprietar Risc	Obs
2.1	Discontinuități de finanțare și fragmentare bugetară anuală	Mediu-Ridicat,	Foarte Ridicat-	CRITIC	MF / MApN / CSAT	
2.2	Pentru finanțarea externă					#
2.3	Întârzieri administrative, birocrăție procedurală și blocaje legislative	Ridicat	Ridicat	CRITIC	Parlament / Guvern	

2.4	Deficit cronic de personal calificat (tehnologii înalte, cyber, C4ISR)	Ridicat	Foarte Ridicat	CRITIC	MApN (SMRU)	
2.5	Dependență strategică externă de furnizori (lipsă autonomie logistică)	Mediu	Ridicat	MAJOR	MApN / MEAT	
2.6	Izolare tehnologică/ Operațională în afara arhitecturii unificate C4ISR	Mediu	Foarte Ridicat	CRITIC	SMAp / STS	
2.7	Capacitate limitată de mentenanță națională (Nivel Depot/Industrial)	Ridicat	Ridicat	CRITIC	MEAT / MApN	
2.8	Vulnerabilități cibernetice și la acțiuni de război electronic (EW)	Mediu-Ridicat	Foarte Ridicat	CRITIC	Comandamentul Cyber	
2.9	Rezistență organizațională la schimbarea culturii de comandă	Ridicat	Mediu-Ridicat	MAJOR	SMAp / Doctrine	

Obs.

Pentru finantarea externă nu este nici-un risc, mai exact riscul e minor. Riscuri SUNT insa pentru fiantarea de la buget a operationalizarii (hale, drumuri, utilitati, sisteme de securitate etc).

3. Analiza Detaliată a Riscurilor și Impactului Operațional

3.1. Riscul Financiar și Predictibilitatea Bugetară

- **Descriere:** Majoritatea programelor finanțate prin SAFE au un caracter multianual complex. Lipsa unui cadru de finanțare multianuală reală, protejat împotriva rectificărilor bugetare conjuncturale, afectează direct graficele de producție ale partenerilor industriali. Bani nu sunt de la buget. Finantarea este externă. Riscurile de a nu primi banii UE sunt minime dacă sunt îndeplinite cerințele. Risc financiar mare este pentru asigurarea de la buget a fondurilor pentru operaționalizare (hale, drumuri, utilitati, sisteme de securitate etc)
- **Impact Operațional:** Decalarea livrărilor, acumularea de penalități contractuale comerciale, renegocieri de preț dezavantajoase din cauza inflației din sectorul de apărare și pierderea credibilității în fața partenerilor strategici din Alianță. Risc de neoperaționalizare in lipsa fondurilor naționale nu a celor de la UE.
- **Recomandare:** Instituirea prin lege a unui mecanism de credite de angajament multianuale intangibile pentru programele SAFE; auditare financiară trimestrială integrată. In lipsa de fonduri nationale, recomandarea unei derulari riguroase este cea mai sigura solutie.

3.2. Riscul de Guvernanță și Management Multidisciplinar

- **Descriere:** Succesul programului SAFE implică un spectru larg de actori instituționali: MApN, Ministerul Finanțelor, Ministerul Economiei (industria autohtonă), autorități naționale de certificare/securitate și companii externe. Absența unei autorități unice de coordonare generează dispararea responsabilității

de aceia conteaza contractele. Nu va face nimeni altceva in plus decât ce s-a semnat.

- **Impact Operațional:** Blocaje administrative la interfața dintre ministere, întâzieri majore în procedurile de recepție, omologare și testare, blocând intrarea în înzestrare a echipamentelor. Testarea, omologarea, recepția o face doar MAPN, de aceia atenția în întocmirea programelor și impunerea corectă a termenelor este esențială.
- **Recomandare:** Înființarea unei Structuri Unice de Coordonare (Task Force Interinstituțional) direct subordonate MAPN cu acces direct la sprijin Guvernamental, cu personal selectat pe criterii stricte de management de program.

3.3. Riscul Asociat Resursei Umane (Capitalul Intelectual Militar)

- **Descriere:** Ritmul de adoptare a sistemelor avansate SAFE devansează capacitatea actuală a sistemului de management al resurselor umane din armată. Sistemele moderne sunt intensive în date și rețele, necesitând competențe înalte care sunt disputate acerb de sectorul privat (IT, Cyber, Robotică).
- **Impact Operațional:** Subutilizarea cronică a tehnologiei cumpărate, degradarea accelerată a echipamentelor prin exploatare incorectă și creșterea dependenței critice de asistența tehnică a contractorului privat, paralizând autonomia forței în teren.
- **Recomandare:** Crearea unui statut special al specialiștilor tehnici din forțele armate, cu grile de salarizare competitive cu piața civilă, respectiv specialiști care derulează fonduri europene; parteneriate academice obligatorii pentru formare accelerată.

3.4. Riscul Logistic, Industrial și Sustenabilitatea Ciclului de Viață

- **Descriere:** O capacitate nu este definită doar de platforma achiziționată, ci de capacitatea de a o menține operațională 20-30 de ani. În prezent, se constată o integrare redusă a industriei naționale de apărare în lanțurile logistice ale marilor furnizori externi. În prima fază este problema operaționalizării. S-a văzut la Patriot. Cu industria sunt obligații contractuale, inclusiv în privința industriei naționale.
- **Impact Operațional:** Vulnerabilitate strategică majoră în situații de criză sau război, când liniile de aprovizionare globale sunt blocate; termene de reparație uriașe și costuri de mentenanță (*Life Cycle Cost*) care pot depăși de 3 ori costul inițial de achiziție.
- **Recomandare:** Condiționarea achizițiilor SAFE de clauze stricte de transfer de tehnologie către centre de mentenanță de nivel Depot (mentenanță majoră) localizate în România. SAFE este exceptat de la offset.

3.5. Riscul de Interoperabilitate, Integritate C4ISR și Izolare Tehnologică

- **Descriere:** Valoarea tactică a noilor platforme tinde spre zero dacă acestea funcționează ca „insule tehnologice”. Miza centrală este conectarea lor nativă într-un spațiu de luptă digitalizat, unificat, conform standardelor NATO (*Joint All-Domain Command and Control*). Depinde ce este scris în contractele deja semnate.
- **Impact Operațional:** Pierderea completă a avantajului informațional, incapacitatea de a partaja date țintă în timp real între categorii de forțe și riscul apariției incidentelor de tip „fratricid” din cauza lipsei integrării datelor.

- **Recomandare:** Regula „C4ISR First” – nicio platformă combatantă nu trebuie achiziționată fără bugetarea anterioară sau simultană a kit-urilor de integrare în rețeaua națională de comandă-control.

3.6. Riscul Cibernetice și Asigurarea Rezilienței Spectrului

- **Descriere:** Digitalizarea masivă adusă de SAFE extinde exponențial suprafața de atac a structurii de forțe. Vulnerabilitățile pot fi exploatate prin atacuri cibernetice asimetrice, acțiuni de bruiaj electromagnetic persistent (EW) sau atacuri asupra lanțului de aprovizionare cu componente software.
- **Impact Operațional:** Pierderea capacității de comandă-control în momentele critice ale operației, alterarea datelor din sistemele de sprijin al deciziei și orbirea senzorială a forțelor în teren.
- **Recomandare:** Integrarea obligatorie a standardelor de securitate cibernetice de tip „Zero Trust” în arhitectura tehnică a tuturor sistemelor din programele SAFE încă din faza de design. Sunt echipamente de raft, deja contractate.

4. Factorul de Succes Decisiv: Tranziția Culturală către "Mission Command"

Analiza strategică demonstrează că bariera principală în calea succesului programelor SAFE nu este una de natură tehnologică, ci una profund cultural-organizațională. Implementarea unor sisteme de arme de generație nouă presupune abandonarea definitivă a culturii instituționale moștenite, caracterizată prin centralizare excesivă a deciziei, rigiditate procedurală și compartimentare rigidă a informațiilor. Pentru a transforma tehnologia avansată în eficiență militară, structura de forțe trebuie să tranșioneze accelerat către modelul doctrinar occidental **Mission Command**. Acest model pune accent pe:

- Descentralizarea controlului și stimularea inițiativei la nivel tactic.
- Execuția descentralizată bazată pe intenția și inițiativa comandantului, nu pe ordine ultra-detaliat.
- O cultură organizațională care acceptă riscul asumat și încurajează fluxul liber al datelor în rețele integrate.

Fără această mutare de paradigmă culturală, tehnologia SAFE va fi folosită sub parametrii săi constructivi, generând doar o iluzie a capacității.

5. Concluzii și Linii de Acțiune Strategice pentru Decidenți

Implementarea programului SAFE reprezintă un test de maturitate instituțională pentru managementul apărării naționale. Pentru a muta în mod real centrul de greutate al dezbaterii naționale de la faza simplistă de achiziție („ce cumpărăm”) la faza esențială de generare de capacitate sustenabilă („cum transformăm investiția”), se propun următoarele linii strategice de acțiune:

1. **Nivel Guvernamental/CSAT:** Legiferarea unui mecanism național integrat de gestionare a capacităților militare (bazat pe ciclul de viață complet al sistemelor) și asigurarea unei protecții bugetare multianuale.
2. **Nivel Legislativ (Comisiile de Apărare):** Corelarea funcției de control parlamentar nu doar cu monitorizarea cheltuirii bugetului, ci cu evaluarea stadiului de operaționalizare (DOTMLPFI) a unităților beneficiare.

3. **Nivel MApN / Statul Major al Apărării:** Accelerarea procesului de reformă a învățământului militar și a doctrinelor tactice, prioritizând digitizarea, interoperabilitatea C4ISR și implementarea reală a principiilor *Mission Command*.

În concluzie, abordarea integrată a dimensiunilor umane, logistice și doctrinare reprezintă singura cale prin care programul SAFE poate deveni, dincolo de un simplu program de înzestrare, un veritabil motor de transformare profundă și modernizare structurală a Sistemului Național de Apărare.

CONSILIUL DIRECTOR CSÎA