

<http://www.luju.ro/cantarea-lui-coldea-pentru-premierul-tudose-iata-ce-laudatio-i-a-facut-premierului-mihai-tudose-fostul-sef-operativ-al-sri-generalul-florian-coldea-lucrarea-aduce-o-certa-contributie-poate-reprezenta-un-reper-sunt-de-apreciat-eforturile-pentru-o-documenta>



**CANTAREA LUI COLDEA PENTRU PREMIERUL TUDOSE – Iata ce laudatio i-a facut premierului Mihai Tudose, fostul sef operativ al SRI, generalul Florian Coldea: „Lucrarea aduce o certa contributie... Poate reprezenta un reper... Sunt de apreciat eforturile pentru o documentare riguroasa... Originalitatea si noutatea abordarii”. Teza de doctorat a lui Tudose a fost garantata si de fostul director al SRI George Maior, care insa a fost ceva mai rezervat in laude (Documente)**

Scris de George TARATA | Data: 27.06.2017 18:42



Premierul Mihai Tudose, propus de PSD-ALDE și desmenat de președintele Klaus Iohannis, l-a dat pe spate cu teza sa de doctorat pe **fostul șef operativ al SRI, generalul Florian Coldea (foto stanga)**. Acesta a fost impresionat de teza de doctorat a lui Mihai Tudose intitulată *“Infrastructura critica – model și strategie managerială”*, pe care a catalogat-o ca fiind un „reper” și un „document de referință”.

Așa cum se știe deja, teza de doctorat a lui Mihai Tudose, susținută la Academia Națională de Informații „Mihai Viteazul” din cadrul Serviciului Român de Informații, conține un laudatio din partea generalului Florian Coldea. Este vorba despre un “Cuvânt-înainte” scris de Coldea, în care acesta își exprimă aprecierea față de lucrarea lui Mihai Tudose.

---

De asemenea, aceeași teza de doctorat a lui Tudose conține și o postfață semnată de **fostul director al SRI George Maior (foto dreapta)**. Totuși, după cum se poate vedea în cele ce urmează, Maior a fost ceva mai rezervat în laude decât Florian Coldea.

“Cuvântul înainte” a lui Florian Coldea și “Postfață” lui George Maior au fost publicate în de jurnalista Sorina Matei.

**Iată “Cuvântul înainte” al generalului Florian Coldea:**

## CUVÂNT-ÎNAINTE

Profundele schimbări economice și tehnologice care au marcat sfârșitul secolului al XX-lea și începutul celui actual au indus modificări substanțiale în registrul riscurilor și amenințărilor la adresa securității, devenind predominante cele asimetrice, neconvenționale și/sau transfrontaliere.

Sistemele vitale pentru funcționarea în condiții de siguranță a vieții economice și sociale – care au cunoscut o dezvoltare tehnologică rapidă și o interconectare accelerată – au intrat progresiv în atenția unor persoane, grupări ori organizații extremiste sau teroriste, care iau în calcul afectarea acestora pentru obținerea unor deziderate sau ca reacție la acțiunile considerate ostile ale unor state sau alianțe regionale/internaționale.

Riscurile la adresa rețelelor de infrastructuri sunt amplificate și de consecințele fenomenului de încălzire globală (precum manifestările meteorologice extreme), de vulnerabilitățile sistemelor tehnologice ori exploatarea deficitară a acestora.

În consecință, protecția acestor sisteme vitale – de a căror funcționare eficientă și fără sincope depinde stabilitatea economică și socială (la nivel național și, uneori, regional), cu atât mai mult în epoca globalizării – a devenit un subiect de maximă actualitate și preocupare atât pentru factorii de decizie și structurile cu responsabilități în domeniul securității, cât și pentru mediul academic. Implicat, orice demers de cercetare științifică asupra subiectului este deopotrivă oportun și necesar. În plus, actualitatea unei cercetări dedicate acestei problematici este reclamată de faptul că demersurile întreprinse la nivel național pentru implementarea



unui sistem adecvat de identificare, desemnare și protecție a infrastructurilor critice sunt, încă, într-o fază incipientă.

Din această perspectivă, lucrarea „*Infrastructura critică – model și strategie managerială*” aduce o certă contribuție atât în plan conceptual, cât și în abordarea managerială a riscurilor din domeniu, la eforturile de realizare a unui mecanism eficient și flexibil de protecție a infrastructurilor critice, în concordanță cu riscurile la adresa acestora identificate la nivel național.

Analiza riguroasă a conexiunilor dintre componenta de securitate și sistemele de infrastructuri, evaluarea detaliată a problematicei – plecând de la definirea conceptelor, studiul infrastructurii critice militare, evidențierea amenințărilor la care sunt expuse acestea etc. –, dar, mai ales, formularea unor opțiuni strategice și a unor sugestii viabile de operaționalizare a unui sistem coerent de protecție sunt doar câteva din argumentele care determină originalitatea și noutatea abordării.

Caracterul ridicat de aplicabilitate al cercetării derivă și din propunerea unui „Model-cadru” pentru managementul securității infrastructurilor critice naționale și europene, care se adresează sectoarelor vizate în mod prioritar – energia, transporturile, comunicațiile și tehnologia informațiilor – cu evidențierea necesității unui mecanism viabil de comunicare inter-instituțional și inter-statal, cu susținere comunitară.

Dintre numeroasele propuneri și soluții pertinente formulate de autor, confirmate de demersuri recente inițiate la nivelul factorilor de decizie, se impune menționarea celei vizând necesitatea stringentă de elaborare a unei strategii naționale care să asigure armonizarea cu legislația europeană și să permită promovarea eficientă și dezvoltarea parteneriatului public-privat, ca mecanism vital pentru configurarea unui sistem funcțional de identificare, desemnare și protecție a infrastructurilor critice. Realitatea a demonstrat, de asemenea, concluzia prezentată în lucrare, conform căreia este imperios necesară dezvoltarea și implementarea unei politici unitare, singura capabilă să asigure îmbunătățirea



capacității de răspuns la potențialele amenințări asupra infrastructurilor critice.

Nivelul teoretico-aplicativ ridicat, bazat pe o bună cunoaștere și un studiu aprofundat al problematicii, sistematizarea eficientă a ideilor, în mod special gradul ridicat de adecvare și consistență al sugestiilor privind managementul acestei categorii de infrastructuri reprezintă argumente solide pentru considerarea lucrării drept un document de referință în domeniu. Lucrarea poate reprezenta, deopotrivă, o lectură extrem de utilă pentru experții implicați în procesului actual de reglementare normativă și doctrinară a problematicii, dar și pentru cei interesați de subiect.

Într-o perioadă de abundență a studiilor despre teme de actualitate pentru securitatea națională, sunt de apreciat eforturile de documentare riguroasă și formularea unor propuneri concrete și pragmatice, care, dincolo de creșterea nivelului de cunoaștere a domeniului abordat, aduc plusvaloare certă demersurilor de implementare a celor mai potrivite soluții pentru situația dată.

Lucrarea de față îndeplinește exigențele presupuse de un astfel de demers și poate reprezenta un reper în perspectiva sincronizării, inclusiv din punct de vedere normativ, a inițiativelor naționale cu preocupările de maximă actualitate existente la nivel comunitar.

Gl. bg. Coldea Florian

Iata "Postfata" fostului director SRI George Maior:

## POSTFAȚĂ

În lucrarea sa, *Infrastructura critică – model și strategie managerială*, Mihai Tudose abordează o problemă importantă a ultimilor ani, care a dobândit o relevanță deosebită pentru securitatea statelor și a cetățenilor. Lumea actuală este una a interconexiunilor, a globalizării clădite pe infrastructuri de comunicare și schimburi de date, pe circulația extraordinar de rapidă a ideilor, bunurilor, persoanelor. Realitatea economică și socială contemporană se bazează, de fapt, pe existența unor infrastructuri critice. În același timp, modul în care înțelegem și utilizăm acest concept poate fi foarte diferit, de la un stat la altul, de la o organizație la alta, pentru că se bazează pe o combinație între tradițiile culturale și instituționale naționale, modul în care a fost realizată trecerea la societăți informaționale postmoderne și capacitățile și sistemele statale de protecție și avertizare timpurie disponibile.

În cadrul teoriilor legate de funcționarea arhitecturilor de rețea (*network architectures*) termenul de infrastructuri critice se referă la acele noduri, puncte inflexiune, zone care sunt fundamentale pentru funcționarea principalelor rețele ce deservește populația într-o anumită regiune. Dacă termenul de „infrastructuri critice” a apărut oficial pe agenda politică doar în 1998 printr-o cunoscută directivă a președintelui Bill Clinton, problematica este însă mult mai veche: în timpul Războiului Rece, Kennedy și Hrușciov au descoperit că un război nuclear s-ar fi putut declanșa în momentul crizei rachetelor din Cuba pentru că nu dispuneau atunci de un sistem de telecomunicații care să le permită să discute direct.

În secolul XXI, protecția infrastructurilor critice, prevenirea disrupției acestora în cazul unor atacuri teroriste sau de altă natură, cyberwarfare sau riscurile generate de catastrofe naturale la adresa acestor infrastructuri sunt deja o problemă majoră, poate



cea mai importantă, a securității internaționale. Vorbim de o problemă cu atât mai vastă cu cât se referă la zone și tipuri de management al crizelor care au fost percepute în trecut ca fiind foarte diferite conceptual: de la atacurile cibernetice la adresa Estoniei de acum câțiva ani, la efectele majore ale norului de cenușă produs de erupția vulcanului islandez acum mai puțin de o lună, sau la potențialul distructiv al unei sistări a livrărilor de energie sau de apă potabilă într-o perioadă de criză. Acestea sunt tot atâtea ipostaze în care statul este chemat în prezent să gestioneze securitatea infrastructurilor și să prevină efecte ce pot fi catastrofale asupra vieții de zi cu zi a cetățenilor săi. Mai mult, în prezent, acest domeniu tinde să devină o temă centrală a cooperării în cadrul securității colective în Alianța Nord Atlantică și un subiect de reglementare comunitară la nivelul Uniunii Europene, pentru că statul, ca actor individual, nu dispune singur de capacitatea de a răspunde unor riscuri la adresa infrastructurilor transnationale, fie acestea de comunicații, energetice sau de transport. Mai mult, efectele unor atacuri sau disruperi ale funcționării infrastructurilor critice se manifestă în cascadă cu implicații care sunt rareori limitate la un singur stat.

De aceea, sistemele de protecție și de susținere a funcționării lor nu pot fi concepute altfel decât printr-o rețea de parteneriate public-privat, național-internațional prin formule de abordare cooperativă transectorială care să definească un set de concepte și de modalități de acțiune unitare și structurate. Fără a aborda în mod integrat aceste concepte, nu se va putea construi un sistem de securitate adecvat, capabil să protejeze individul împotriva unor amenințări atât de diverse și de complexe precum cele existente în lumea secolului XXI: de la terorism la atacuri cibernetice, de la efectele unui nor vulcanic asupra transporturilor europene și până la disruperea furnizării de energie, dezastrele ecologice sau pandemile. Securitatea înseamnă în primul rând identificarea și managementul riscului, cunoașterea și strategia care îți permite să transformi această cunoaștere în acțiune.

George Cristian Maior  
Director Serviciul Român de Informații