



**COLOCVII CÆSAR |**

**TEHNOLOGIA INFORMAȚIEI I**

**SECURITATE CIBERNETIC**

**HiTech**  
**CÆSAR**

# ROMÂNIA 2030 | TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETIC

## OBSTACOLE. SOLUȚII. ASUMARE ȘI RESPONSABILITATE

Cea de-a doua ediție din seria colocviilor derulate în cadrul **Centrului pentru Acces la Expertiza Studenților și Absolvenților Români (CÆSAR)** a reunit la Institutul Bancar Român peste 50 de profesioniști din domeniile IT și securitate cibernetică – tineri antreprenori, cercetători, experți, reprezentanți ai mediului privat și persoane cu rol decizional sau de conducere din industriile științelor tehnice. Printre invitații de onoare s-au numărat: **Alexandru Borcea**, Președinte ARIES (Asociația Română de Industrie Electronică și Software), **Justin Capr**, inventator și inginer român, **Călin Rangu**, Președinte al Institutului pentru Managementul Capitalului Intelectual și al Schimbării și Strategic Alliance Manager pentru grupul internațional de consultanță AREOPA, precum și **Zoltán Somodi**, Director General la Matrix Business Consulting, care a ocupat funcția de Secretar de Stat pentru Tehnologia Informației, în cadrul Ministerului Comunicațiilor și Tehnologiei Informației.

În înfrunirea de deschidere a colocviului, Domnul Justin Capr și Domnul Călin Rangu despre importanța definirii unor măsuri necesare pentru facilitarea contribuției fiecăruia dintre noi la procesele de dezvoltare a României.

**Colocviul CÆSAR HiTech** și-a propus abordarea unor domenii inovatoare, de importanță strategică pentru România: Tehnologia Informației și Securitatea Cibernetică. Acest eveniment a avut ca scop construirea bazelor unor direcții strategice de dezvoltare a țării noastre în domeniile vizate prin identificarea principalelor probleme existente, a unor soluții viabile și a unor modalități de implementare realiste.

Concluziile grupurilor de expertiză invitate –**Tehnologia Informației (IT) și Securitate Cibernetică (CYBER)** – reprezintă un prim pas important în această direcție. Ceea ce urmează este materializarea soluțiilor identificate în proiecte concrete, de impact pe termen mediu și lung.

**Liga Studenților Români din Străinătate (LSRS)** adresează mulțumiri celor doi moderatori ai grupurilor de expertiză, Domnului Zoltán Somodi și Domnului Călin Rangu, tuturor participanților, precum și voluntarilor LSRS care au contribuit la organizarea acestui eveniment.



# OBSTACOLE ȘI SOLUȚII

Grupurile de expertiză „Tehnologia Informației” (IT) și „Securitate Cibernetică” (CYBER) au identificat o serie de obstacole care frânează dezvoltarea acestor domenii în România și au dezvoltat o serie de soluții menite să răspundă la acestea.

## TEHNOLOGIA INFORMAȚIEI

### Obstacole

- I. Colaborarea precară a informaticienilor din România atât în interiorul țării, cât și cu partenerii externi. Nu există un cadru organizat (de tipul unui „cluster”, de pildă) care să poată coagula comunitatea informaticienilor români, indiferent de frontiere.
- II. Slaba performanță a asociațiilor din domeniul IT în termeni de vizibilitate, atractivitate și activitate
- III. Lipsa unei viziuni coerente și pe termen lung pentru dezvoltarea domeniului IT din România, agreată la nivel public, privat și neguvernamental
- IV. Caracterul limitat și discontinuu al inițiativelor în antreprenoriatul IT, extrem de necesare pentru accelerarea dezvoltării acestei industrii
- V. Migrația resurselor umane valoroase („brain drain”)
- VI. Numărul limitat al finanțărilor disponibile pentru acest sector
- VII. Inadaptarea programei educaționale din domeniul IT la cerințele actuale și nivelul în general slab de pregătire a cadrelor didactice. Mai mult, mediul universitar nu încurajează colaborarea.
- VIII. Lipsa frecvent întâlnită a unei finalități practice a proiectelor de cercetare din domeniul IT și slaba reprezentare a laturii de cercetare în multe proiecte de antreprenoriat. Este nevoie de o corelare a acestora: aplicarea cercetării în antreprenoriat și invers.

### Soluții

- I. Implementarea standardului EURES (EUropean Employment Services) în România, prin Agenția Română de Asigurare a Calității în Învățământul Superior (ARACIS)



## PARTICIPANȚI

Adrian Bîzgan  
Adrian Socaciu  
Alexandru Borcea  
Alexandru Căbuz  
Alexandru Rada  
Ana Maria Andronic  
Andrei Hodorog  
Andrei Savu  
Aurelian Popa  
Bogdan Alexandrescu  
Bogdan Marchidanu  
Cătălin Profir  
Claudiu Morariu  
Florin Munteanu  
Iulian Popescu  
Mihai Nad  
Ionuț Munteanu  
Maria Alecu  
Marius Mocian  
Simona Iconaru  
Sorin Dinea  
Ovidiu Moise  
Ovidiu Nisioiu

## MODERATOR

Zoltán Somodi

## ORGANIZATORI

Diana Arhir

Dan Nechita

## RAPORTORI

Andrei Polmolea

Andrei Stan

- II. Crearea și dezvoltarea unui Forum online pentru coagularea comunității informaticienilor din România, începând cu acest grup de expertiză
- III. Stabilirea de parteneriate între asociații IT și instituțiile din mediul universitar și post-universitar românesc
- IV. Crearea unui „cluster” de informaticieni care să reunească 500 de profesioniști internaționali, cu rol de advocacy/lobby și consultant : Creative Professionals Worldwide
- V. Seminarii de dezvoltare pe diverse teme legate de IT și inovare (de exemplu, despre „clustering”, despre noua paradigmă a învățării, despre fonduri structurale etc.) organizate de membrii acestui grup de expertiză
- VI. Derularea unor evenimente periodice de tip „Open Coffee”, în care antreprenori în IT își prezintă ideile de afaceri
- VII. Crearea unui Birou de Transfer Tehnologic, care să poată conecta cercetători și formatori cu antreprenori și furnizori de servicii. Institutul European de Tehnologie este un bun exemplu în acest sens.

# SECURITATE CIBERNETIC

## Obstacole

- I. Caracterul incomplet al cadrului legislativ ce reglementează activitatea din domeniul securității cibernetice
- II. Insuficienta dezvoltare a structurilor publice specializate în depistarea breșelor de securitate
- III. Aplicarea deficitară a legii în materie de sancțiuni corespunzătoare activităților ilegale din spațiul cibernetic
- IV. Cooperarea internațională redusă în materie de securitate cibernetică în contextul mai larg al asigurării securității naționale
- V. Slaba conștientizare a oamenilor (mai ales a adulților de peste 40 de ani) în privința riscurilor pe care le implică insecuritatea cibernetică și utilizarea imprudentă a rețelelor sociale
- VI. Managementul limitat al riscurilor în materie de securitate cibernetică, care face ca măsurile de securizare să fie luate deseori reactiv, după incidente
- VII. „Hactivismul” ca formă de protest ce pune în pericol securitatea cibernetică a instituțiilor publice și private

## Soluții

- I. Amendarea cadrului legislativ printr-o lege a *hacking-ului* etic și prin norme care să permită înființarea unor structuri private de identificare a incidentelor cibernetice
- II. Dezvoltarea structurilor publice care activează în domeniul protecției infrastructurilor cibernetice. Un bun început în acest sens este înființarea în 2011 a Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), care are nevoie de consolidare instituțională și de îmbunătățire comunicării cu centrele de tip CERT de la nivel teritorial.
- III. Dezvoltarea unor structuri private pentru prevenirea, analiza și identificarea incidentelor cibernetice care să fie în strânsă colaborare cu structurile publice cu competență de reacție la astfel de incidente. La nivel financiar-bancar, Banca Națională a României poate avea un rol esențial în stimularea instituțiilor bancare private să înființeze centre de tip CERT specializate și să se asigure de o bună comunicare între acestea



## PARTICIPANȚI

Adelina Palade  
Adrian Păuna  
Ana Mihaela Andrei  
Ana Cobzaru  
Andrei Adoamnei  
Bogdan Condurache  
Corneliu Grigore  
Dana Andronie  
Dan Dimofte  
Dan Tofan  
Dinu Smadu  
Gabriel Țuțu  
Ionuț Andronache  
Ionuț Popescu  
Ionuț Ciocârlie  
Maria Zamfir  
Oana Costea  
Stelian Stancu  
Victor Vevera

## MODERATOR

Călin Rangu

## ORGANIZATORI

Diana Arhir

Dan Nechita

## RAPORTORI

Alexandra Sasu

Maria-Magdalena Manea

- IV. Înființarea unui Central Informatics Organization (CIO) Office, ca agenție guvernamentală, cu rol în coordonarea integrării programelor de IT și de securitate din sectorul public
- V. Deschiderea unor centre profesionale pe lângă instituțiile de învățământ superior relevante, care să ofere servicii în materie de depistare a breșelor de securitate și care să permită studenților să-și exerseze și să-și dezvolte competențele
- VI. Crearea unui corp de experți judiciari și extrajudiciari specializați în domeniul infracțiunilor informatice care să acorde sprijin parchetelor și instanțelor în rezolvarea cazurilor privind activitățile ilegale din spațiul cibernetic
- VII. Participarea structurilor publice competente în cadre de cooperare internațională —formale și informale—în domeniul protecției, siguranței și securității infrastructurilor critice
- VIII. Campanii de informare, conștientizare și educare a tinerilor în materie de securitate cibernetică în licee și universități, cursuri de inițiere a adulților în tehnologia informației și securitatea cibernetică în instituții publice și centre de formare profesională. Este nevoie de conștientizarea riscurilor la care se expun utilizatorii (indivizi, instituții publice, companii) prin publicarea, divulgarea datelor personale pe rețelele sociale.
- IX. Îmbunătățirea la nivelul companiilor și instituțiilor publice al managementului riscului în materie de securitate cibernetică. Este nevoie de aplicarea unor standarde minime obligatorii în domeniu și de creșterea calității de ansamblu a auditurilor efectuate. În acest sens, este binevenită creșterea profesionalizării auditorilor financiar-bancari.
- X. Reglementarea „hactivismului” la nivel internațional și național