# Reziliența cibernetică și investiția în securitate cibernetică

## din perspectivă economică

**16 octombrie 2025**

**- București -**

*dr.ing. Ruxandra RÎMNICEANU*

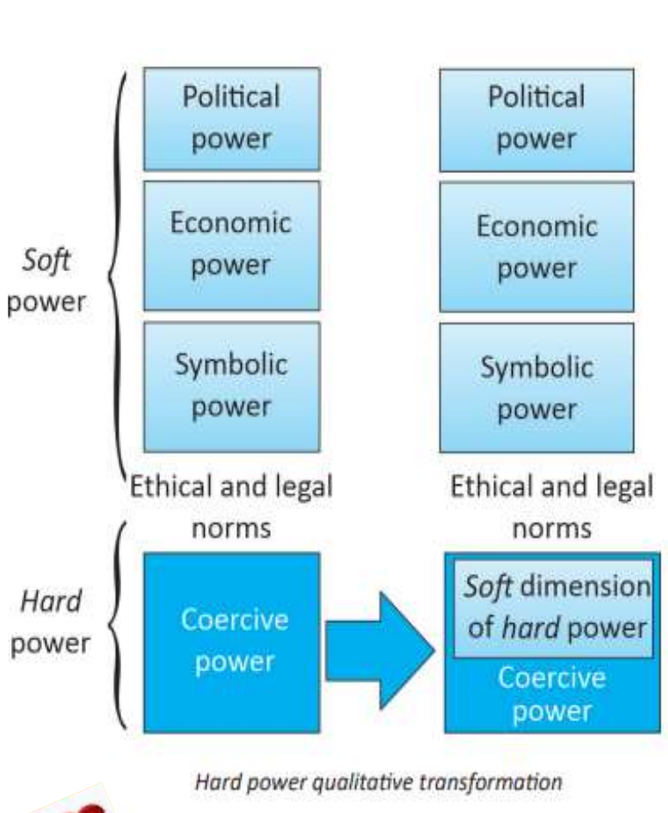
*Consultant strategie*

**Banca Națională a României**

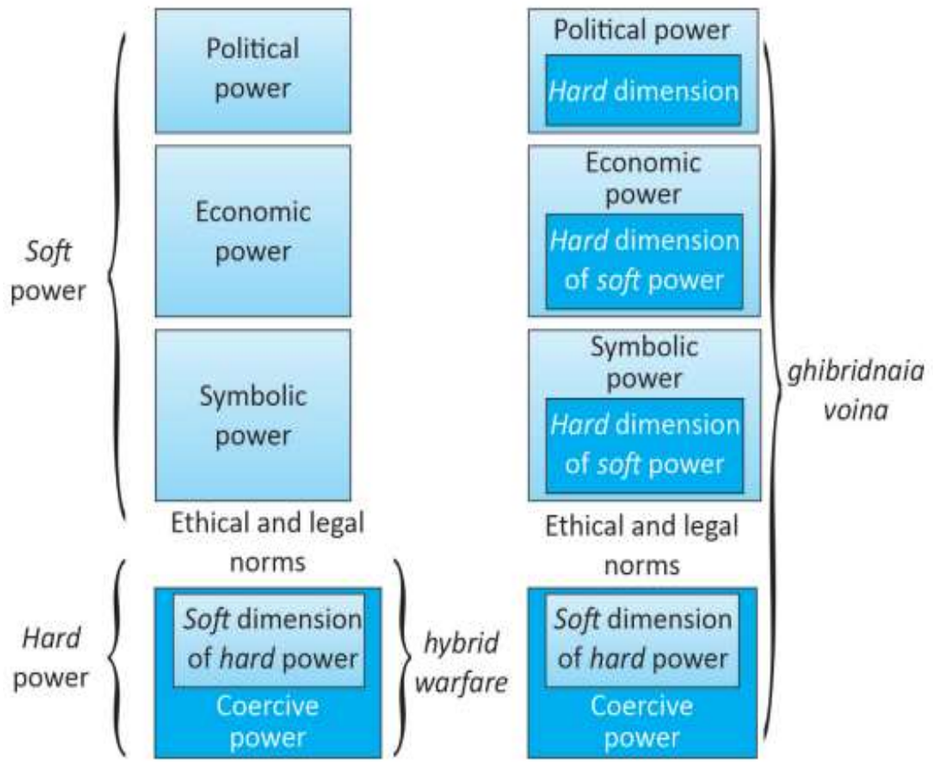

# REZILIENȚA (CIBERNETICĂ) LA AMENINȚĂRILE HIBRIDE

- ***Noua paradigmă a războiului hibrid* (Hoffmann, 2007)**
  - "*fuziunea efectelor acțiunilor convenționale și neconvenționale*"

**„atacuri hibride"** - **art.5** al Tratatului NATO prevede că **"UN ATAC MILITAR ASUPRA UNUI ALIAT ESTE UN ATAC ASUPRA TUTUROR"**




*Hard power qualitative transformation*




: *The two forms of hybrid confrontation*

**Ambiguitatea și disimularea doctrinară a lui Gherasimov** (2013-2019)

- ***un război absolut***
- ***a ignorat rigorile cadrului juridic internațional aplicabil* *până în acel moment***

❖ **a acoperit zona neclară a *„războiului insurecțional"* al lui Messner,** bazat pe șapte metode subversive:


**Putin - metoda *„pompierului incendiar"***

2023

- Poliția și Serviciul Federal de Securitate al Rusiei (FSB) au dobândit noi **capacități de snooping (= "ascultarea în rețea" / "atac cu urechea" - obținerea accesului la date sau informații sensibile prin prezentarea drept sursă de încredere)**, concentrate pe **utilizarea de zi cu zi a telefoanelor și site-urilor**
- instrumentele oferă modalități de **urmărire a anumitor tipuri de activități pe aplicații criptate,** precum WhatsApp și Signal, **monitorizare a locațiilor telefoanelor, identificare a utilizatorilor anonimi** pe rețelele sociale și **spargerea conturilor cetățenilor**

**premise *"atacuri hibride"***

- ***„sabotarea felului de viață european"***
- ***acte de sabotaj la* Infrastructuri critice** precum ***conducte, cabluri de date sau sisteme prin satelit și la* servicii vitale** (ex. **oct.2022 - Germania**, când „cineva" a tăiat cablurile care asigurau **funcționarea sistemului feroviar** din nordul țării - ***suspendare*** *mersul trenurilor în nordul țării timp de* ***aproximativ trei ore***)

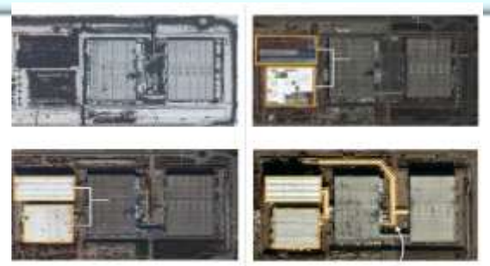
# REZILIENȚA (CIBERNETICĂ) LA AMENINȚĂRILE HIBRIDE


## Industria de supraveghere digitală din Rusia

**Rusia** - a dezvoltat o **industrie proprie de noi instrumente de supraveghere digitală (controlul Internetului, interceptarea convorbirilor și a mesajelor necriptate, accesarea camerelor web, arhivarea traficului ș.a.)**

- a încercat să le vândă în **Europa de Est, Asia Centrală, Africa, Orientul mijlociu și America de Sud**
- **monitorizează camerele de supraveghere instalate în cafenele** ucrainene (**nu pe cele din locuri publice**) **pentru a observa** convoaiele și trenurile care livrează ajutoare
- **furnizează Iranului arme cibernetice**, inclusiv instrumente de supraveghere digitală (tip Protei), **pentru a obține** de la Teheran **dronele** relativ ieftine și eficiente pe care le folosește pentru **a lovi infrastructura ucraineană**
- **a construit cu Teheranul fabrica de drone Yelabuga** (este o fabrică de vehicule aeriene fără pilot și de muniție în zona economică specială Alabuga, lângă Yelabuga, Republica Tatarstan, Rusia, operată de compania rusă Albatross). Ea dezvoltă drone pentru uz militar în invazia rusă a Ucrainei și **are în mare parte studenți, inclusiv minori**

**Deschisă iulie 2023**



**Decembrie 2024** – distrus un depozit de drone Shahed din Tatarstan, fiind distruse componente pentru drone în valoare de 16 milioane de dolari

### Sistemul pentru Activități de Investigații Operative - SORM (1996)

- **program de supraveghere** al Serviciului Federal de Securitate (FSB), **comparabil cu programul de supraveghere PRISM**
- după invazia Ucrainei – extins **la nivelul întregii populații** pentru **a suprima opoziția internă față de războiul din Ucraina** (monitorizarea activității on-line a cetățenilor)

### Kommersant (sept.2017)

- sistem sofisticat de **recunoaștere facială din Moscova** (al șaptelea cel mai supravegheat oraș din lume, cu un număr estimat de **peste 217.000 de camere, din totalul celor 21 de milioane** de camere de supraveghere din întreaga Rusie)

## Manipulare / dezinformare

- folosește spioni, rețelele sociale și mass-media de stat ruse, precum și alte mecanisme închise și ascunse – rețele de influență și proxy - pentru **a eroda încrederea publicului în integritatea alegerilor democratice** din întreaga lume (Reuters), **a intimida lucrătorii electorali**, **a organiza proteste în ziua alegerilor** și "***a sabota votul din străinătate***" (tehnici utilizate încă din 2020)
- în perioada **2020-2023**, ar fi "manipulat" încrederea publicului în cel puțin **11 alegeri din nouă democrații, inclusiv în Statele Unite și în alte 17 state** cu eforturi "mai puțin pronunțate".


**sept. 2015**

**Sistemul de război electronic Krasukha (EW)**

*Sursa: Concern Radio-Electronic Technologies*

- cel mai modern **sistem electronic de război împotriva Siriei** – Krasukha-4 sau Belladona – unitate mobilă **pentru a neutraliza sateliții de spionaj** de pe orbita LEO, cum ar fi seria SUA Lacrosse / Onyx, **radarele de supraveghere aeropurtate și ordonanțe ghidată de radar** la distanțe între 150 și 300 de km
- **capabil să provoace daune sistemelor de comunicații și undelor radio** ale inamicului
- acționează prin crearea unui **bruiaj puternic la frecvențele radar** de bază și ale altor surse care emit unde radio

**Bruiajul act de spionaj și intimidare**

**Rusia operează un război electronic care este activ inclusiv în zona de Est a României**

**mai 2024**

*Sursa: Centrul Euro-Atlantic pentru Reziliență*

# REZILIENȚA (CIBERNETICĂ) LA AMENINȚĂRILE HIBRIDE

**Coreea de Nord, văzută noaptea din spațiu, față de China sau vecinii de la sud**

*Sursa: Stația Spațială Internațională (**2014**)*

**21 febr. 2025**

**Jaful de la Bybit**
***- bursa de criptomonede din Dubai -***

Hackerii din Coreea de Nord **au furat suma record de 1,5 miliarde de dolari în criptomonede**, într-o singură lovitură

- ❑ finanțare **Research Center 227** - *"dezvoltarea de tehnologii și programe de hacking cu scop ofensiv"*
- ❑ *finanțare* ***programe nucleare și de rachete prin hacking***

**...u compromis computerul unui dezvoltator care lucra pentru un furnizor de software pentru portofel digital**

## Coreea de Nord

- a apărut în **1948, în urma haosului** de la sfârșitul celui de-Al Doilea Război Mondial, prin separarea de Coreea de Sud, iar **Uniunea Sovietică a preluat controlul în Nord**, în timp ce Statele Unite au obținut controlul în Sud

- se situează printre **cele mai sărace 66 națiuni** din lume (**2022**)

- Guvernul nord-coreean **controlează toate mijloacele de informare**:
  - deține monopolul asupra tuturor instituțiilor de presă din țară, iar **cetățenilor nu li se permite accesul la surse de știri străine**
  - există **doar trei posturi de televiziune**
  - **accesul la Internet este puternic restricționat.** Majoritatea nord-coreenilor nu au acces la internet, iar cei care au acest privilegiu sunt **autorizați să viziteze doar un număr limitat de site-uri controlate de guvern**

## „Armata cibernetică" a lui Kim Jong Un

- **una dintre cele mai puternic militarizate națiuni din lume,** cu aproximativ 1,2 milioane de militari, potrivit CIA World Factbook
- toți cetățenii efectuează [illegible]
- înființare **Core Computer Center în 1990**
- hackerii din Coreea de Nord **("Lazarus")** au avut roluri de prim rang în câteva lovituri larg mediatizate, cum ar fi
  - atacul asupra **Sony Pictures**, din **2014** (în urma filmului „The Interview" în care era ironizat liderul nord-coreean)
  - în **2016** au reușit să fure 81 de milioane de la **Banca Națională din Banghladesh**
  - episodul **WannaCry**, în **2017**

- tinerii nord-coreeni - **maeștri în infracțiunile informatice financiare, mai ales când este vorba despre furtul de criptomonedă**

- statul asiatic are și un **institut de cercetări în AI** (din **2013**) și colaborează cu experți militari chinezi, pentru **dezvoltarea de noi tehnici și metode în domeniul „machine learning"**
- **copii de cinci ani sunt recrutați și transformați în soldați cibernetici, fiind trimiși la specializare în China și Rusia**

„***amenințare asimetrică***" - o națiune mică și disperată, săracă, poate **ajunge în tăcere în căsuțele de e-mail și în conturile bancare ale bogaților** la mii de kilometri distanță. Ei pot exploata acel acces **pentru a face ravagii în viața economică și profesională a victimelor lor**. Aceasta este **noua linie de front într-un câmp de luptă global**

*Sursa: Geoff White și Jean H Lee, BBC*

| BIPOLARISM | HAOS | POST-HAOS | NOUA ORDINE |
|---|---|---|---|
| xxxxxxxxxxxxxx<br>xxxxxxxxxxxxxx<br>xxxxxxxxxxxxxx | x yttty ttty cd xtttt y yytytyy tttt y tt x<br>xr p u txttd uxett r td g f yy yy<br>xdttsfrtthbxc ty tttt xx ttttt u tt y tt x<br>yyytyx x y x y ttuh yyttoih ouytt aiottre<br>upogu oyts ouy adtw x yytyyy t x y y<br>ttxxxxx y y ctdf er ntf v yytyyyb h r<br>a tt r eet sdr iyer sotctra o c yyyy cre<br>y yyty tr yyy iu yyytyyy u trdtesttt r x t | yyyyyyttyyxvx<br>xyyxyyttyyyyx<br>yy yyyyy yxyy<br>yx yyyyyx yyx<br>yyy yyyyyy yy<br>x yy yxvyy yx<br>y yyyyyyt yy y<br>yy yyxyttxyyy | yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy<br>yyyyyyyyyyyyyyyyyyyy |
| yyyyyyyyyyyyyy<br>yyyyyyyyyyyyyy<br>yyyyyyyyyyyyyy | | | |
| Nealiniaţi | | | |

**22.07.2022**

**„Se apropie o eră nouă"**

**Putin - Forumul *„Idei puternice pentru un nou viitor"*, Moscova.**



x = comunism y = societate democratică de tip occidental (noua ordine) s…r… = accidente t = terorism

# REZILIENȚA INFRASTRUCTURILOR CRITICE / CIBERNETICĂ

**REZILIENȚA** = o măsură a capacității unui sistem de a continua să funcționeze făcând față modificărilor variabilelor de stare, de conducere, precum și parametrilor săi

**(C.S. Holling, 1973**
**"*Resilience and stability of ecological systems*"**
**Institute of Research Ecology, Vancouver, Canada)**

**Studiu asupra definițiilor de reziliență (din diferite perspective disciplinare)**

**(Francis & Bekera, 2014)**

**rezilienta tehnică**

- capacitatea **sistemului fizic al organizației** de **a se comporta în mod corespunzător** în cazul unei crize

**rezilienta organizațională**

- capacitatea **managerilor** care se ocupă de criză **să ia decizii și măsuri** care **să conducă la evitarea** unei crize sau de **a reduce impactul** acesteia

**rezilienta economică**

- capacitatea **entității** de **a face față costurilor suplimentare** care apar dintr-o criză

**rezilienta socială**

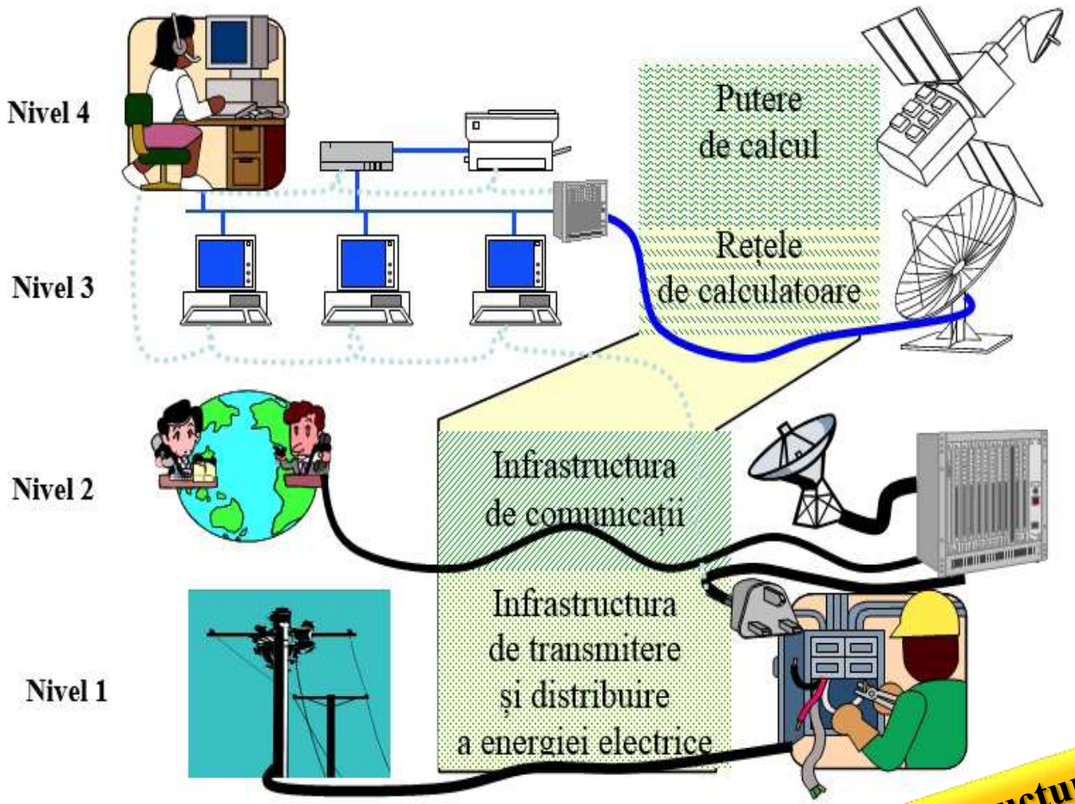
- capacitatea **societății** de **a reduce impactul** unei crize, de **adaptare prin ajutorarea** primelor persoane care intervin sau celor care acționează în calitate de voluntari

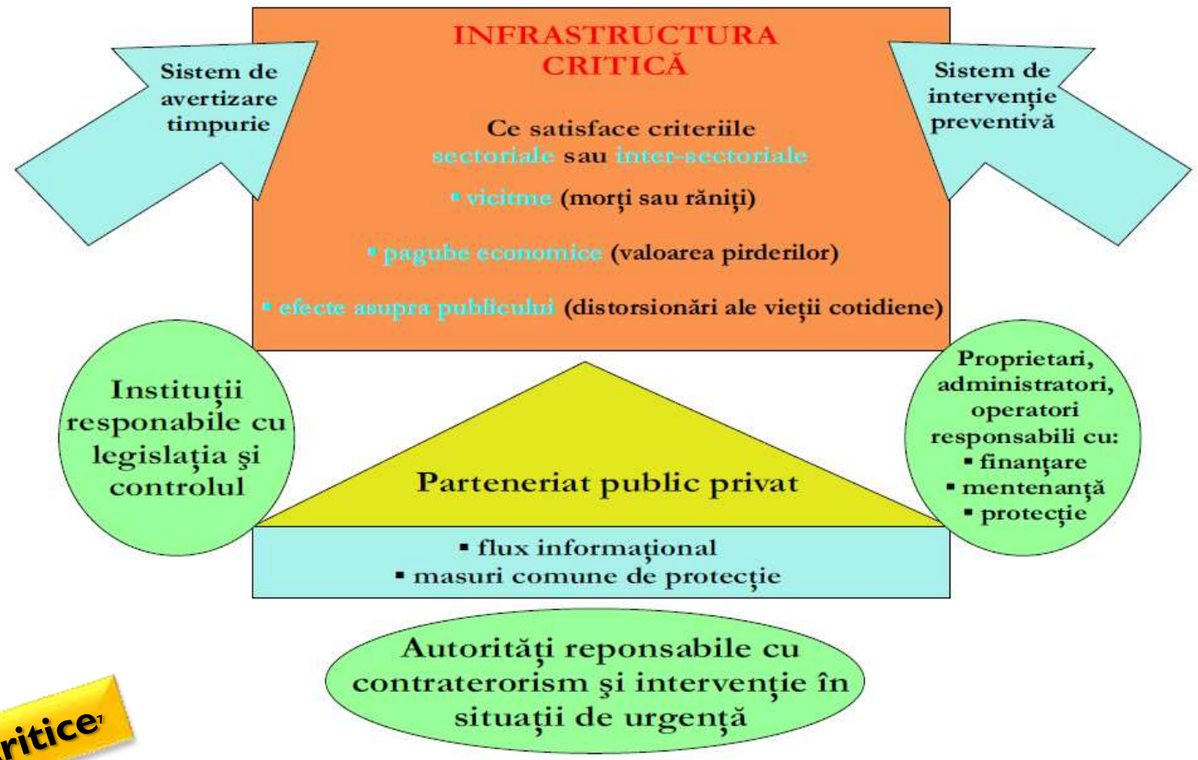
- **11 septembrie 2001**
  - autoritățile de reglementare s-au concentrat inițial pe **recuperarea și reluarea activității Infrastructurilor esențiale ale Pieței Financiare (FMI)** pentru **sistemele de plată en-gros de importanță sistemică**
  - extinderea activității bancare (de exemplu, serviciile bancare pentru **persoane fizice**, precum și pentru alte **companii în afară de FMI**)
- **criza financiară din 2008**
  - **reziliența și viabilitatea sectorului financiar** de a rezista în **condiții severe de stres** și **contagiune a pieței**
  - autoritățile de reglementare din lume s-au concentrat pe **a asigura reziliența financiară** – prin intermediul unei **extinderi notabile a sferei de cuprindere** și **a rigurozității cerințelor de lichiditate, capital, recuperare și rezoluție** – ca **răspuns la amploarea și impactul sistemic** al crizei
- **reziliența operațională și tehnologică (2019)**
  - **gestionarea riscurilor asociate** cu:
    - complexitatea operațională creată de **dependența** din ce în ce mai mare a companiilor **de tehnologiile emergente** (**FinTech** și **BigTech**)
    - **întreruperile** extrem de mediatizate ale **firmelor de servicii financiare din SUA și UK**
    - preocupările legate de **vulnerabilitatea companiilor** în fața **atacurilor cibernetice**
  - **îmbunătățirea rezilienței întreprinderii** este o cerință esențială pentru ca **organizațiile** să rămână **competitive**, să își mențină **nivelul de încredere pe piață** și să sprijine **stabilitatea financiară**

**REZILIENȚA INFRASTRUCTURILOR CRITICE** = capacitatea de **a reduce amplitudinea** și/sau **durata unor evenimente perturbatoare**, prin **potențialul** de **a anticipa**, de **a absorbi**, de **a se adapta la situație** și/sau de **a își reveni rapid**, în urma apariției unui eveniment perturbator

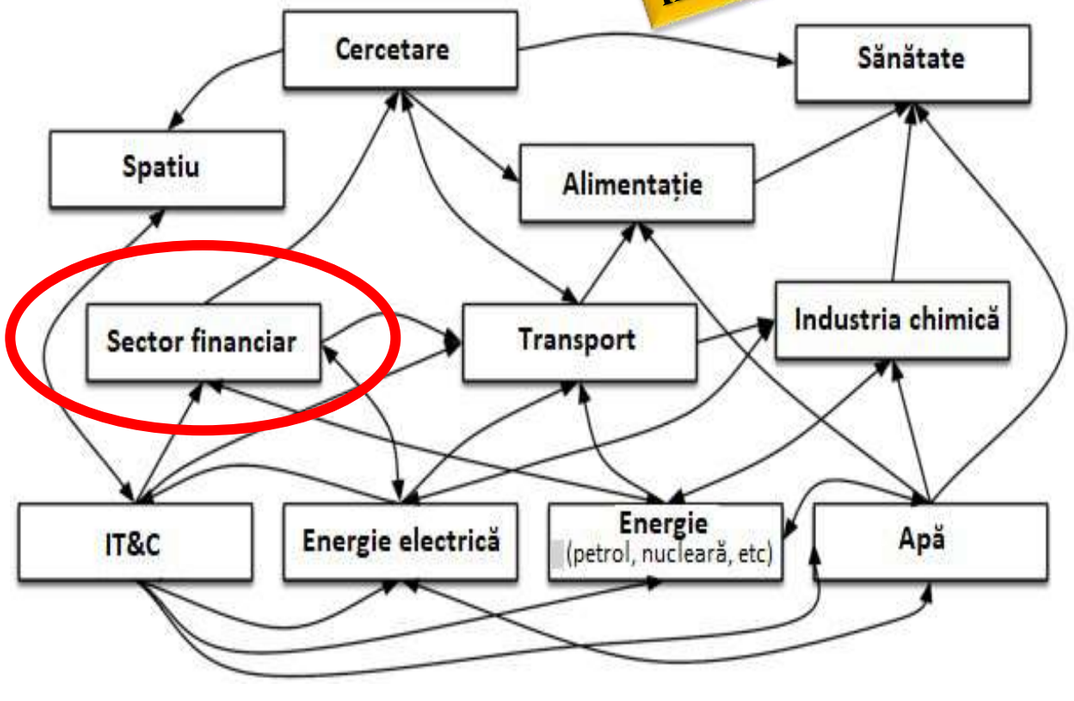
**(Directiva UE 2008/114/CE / OUG nr.98/2010**
**NIAC - National Infrastructure Advisory Council, 2010)**

# REZILIENȚA INFRASTRUCTURILOR CRITICE / CIBERNETICĂ




**interdependența infrastructurilor critice**




**1 fizice:**
2 ICN/ICE sunt (inter)dependente fizic dacă furnizarea serviciului esențial al uneia depinde de producția / materialele / serviciile celeilalte ICN/ICE. Interdependențele fizice apar din legăturile fizice sau conexiuni între elementele infrastructurilor.

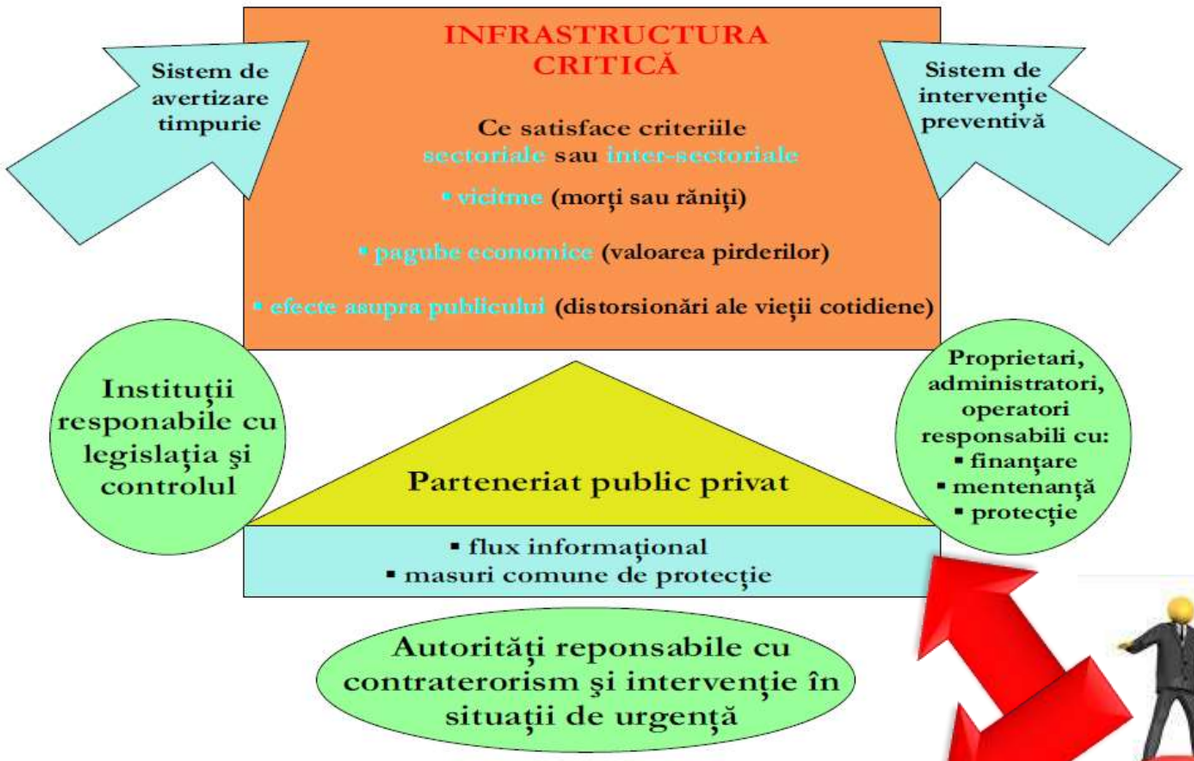
**2 informatice:**
o ICN/ICE se află în relație de (inter)dependență informatică cu o altă ICN/ICE dacă furnizarea serviciilor esențiale ale acesteia depinde de informațiile transmise prin infrastructura IT a celeilalte ICN/ICE.

**3 geografice:**
două ICN/ICE sunt (inter)dependente geografic dacă un eveniment local legat de mediu se produce și influențează gradul de asigurare a serviciilor esențiale la ambele infrastructuri. Aceasta implică o apropiere spațială strânsă a elementelor diferitelor infrastructuri, cum ar fi elementele colocate ale infrastructurilor diferite într-un drept comun de drum.

**4 logice:**
două ICN/ICE sunt (inter)dependente logic dacă starea fiecăreia depinde de starea celeilalte prin intermediul unui mecanism care nu este o conexiune fizică, informatică sau geografică.

**5 sociale:**
starea unei ICN/ICE este afectată de răspândirea tulburării la o altă ICN/ICE legat de activitățile umane (de exemplu, apariția și difuzarea comportamentelor colective care au un impact negativ asupra capacității infrastructurii care urmează să funcționeze).

# REZILIENȚA INFRASTRUCTURILOR CRITICE / CIBERNETICĂ




**în viitor, oricât de bine ar fi pregătite, se va produce totuși o perturbare**

| Perioade de timp | Pași în managementul rezilienței | Fazele rezilienței |
|---|---|---|
| *Înainte de perturbare* | Definirea sistemului ↓ Evaluarea rezilienței ↓ Consolidarea rezilienței | Pregătire Prevenire Protecție |
| *Pe timpul perturbării* | Menținere | Atenuare Absorbție Adaptare |
| *După perturbare* | Restaurare | Răspuns Recuperare |
| | Transformare | Învățare |

**Rolul rezilienței în sisteme**
(Igor Linkov și Benjamin D. Trump, 2019
- *The Science and Practice of Resilience*, Springer, Elveția)


- **Prevenirea incidentelor:**
  - Măsuri de securitate pentru a proteja sistemele și datele de accesul neautorizat
- **Detectarea atacurilor:**
  - Monitorizarea sistemelor pentru a identifica amenințări și activități suspecte
- **Răspunsul la incidente:**
  - Planuri și proceduri pentru a acționa rapid și eficient atunci când are loc un atac
- **Recuperarea după incidente:**
  - Capacitatea de a-și reveni din funcționare și a restabili operațiunile după un eveniment de securitate, limitând pierderile

**Planificare**

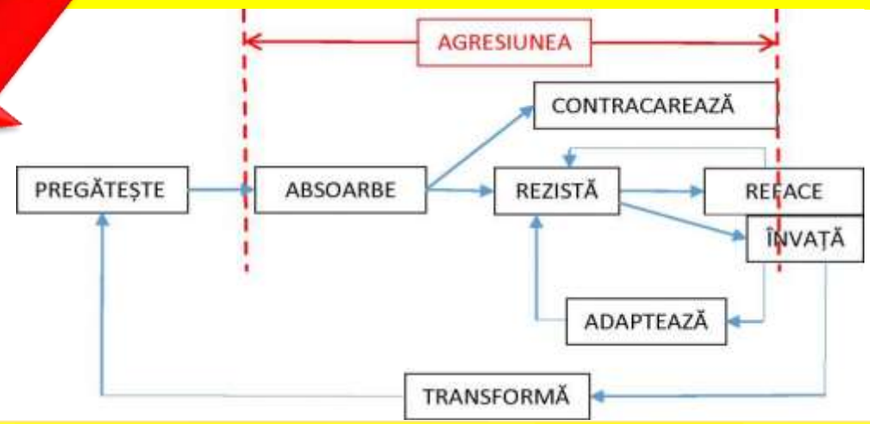
- **Protecția datelor:**
  - Asigură protecția informațiilor sensibile, a datelor personale și a activelor digitale
- **Continuitatea afacerii:**
  - Permite organizațiilor să își continue activitatea chiar și după un atac
- **Reducerea riscurilor:**
  - Limitează impactul financiar și operațional al incidentelor cibernetice

**Impact**

sistem de alertă
mecanism pentru
situații de urgență

**REZILIENȚA CIBERNETICĂ** = capacitatea unui sistem sau a unei retele informatice (organizație) de **a preveni**, **detecta** și **răspunde la atacuri cibernetice** și alte **incidente de securitate**, **minimizând** astfel **impactul** acestora **asupra funcționării normale**
***(Regulamentul UE 2021/694 privind solidaritatea cibernetică***
***Regulamentul (UE) 2024/2847 privind reziliența cibernetică***
**6 iunie 2025 - Plan de acțiune pentru o mai bună gestionare a crizelor și incidentelor cibernetice)**

**optimizarea unor resurse limitate cu scopul de a pregăti sistemele pentru confruntarea cu o largă varietate de amenințări**




**Modelul funcțional al rezilienței în domeniul militar**

# GUVERNANȚA DE SECURITATE CIBERNETICĂ
# LA NIVEL NAȚIONAL

**2021-prezent**

## Implementarea strategiei de securitate cibernetică la nivel național (în plan proactiv / reactiv)

**Consiliul Operativ de Securitate Cibernetică (COSC)**

**raportează CSAT**

funcţia de coordonator tehnic al COSC este asigurată de către **Centrul Naţional Cyberint (CNC)**

**Grupul de Suport Tehnic (GST)**

format din reprezentanţi la nivel de **expert din cadrul instituţiilor sistemului de securitate naţională** reprezentate în cadrul COSC

**Centrul Naţional Cyberint (CNC)** din cadrul Serviciului Român de Informaţii

**informează operativ COSC** cu privire la apariţia incidentelor cibernetice care pot aduce atingere securităţii naţionale

**punct de contact pentru relaţionarea cu organismele similare din străinătate**, în caz de atac cibernetic asupra securităţii cibernetice a României

**Directoratul Național de Securitate Cibernetică (DNSC) - OUG. 104/2021**

a preluat **atribuțiile fostului Centru Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO** (înființat prin HG 494/2011**), inclusiv atribuțiile de Autoritate Competentă la Nivel Național pentru Securitatea Rețelelor și Sistemelor Informatice**

**Legea 294/2024**

**OUG 155/2024**

**punct naţional de contact şi echipă CERT/CSIRT naţională**

- **a) stabilesc** pentru entităţile critice **obligaţii** menite să le sporească reziliența şi capacitatea de a furniza pe piaţa internă servicii esenţiale **b) stabilesc norme** privind supravegherea entităţilor critice şi asigurarea respectării legii
- **cooperează** în baza ***Strategiei privind reziliența entităţilor critice*** (v. art.4 alin.(3) cu **CNCPIC** şi **autorităţile competente responsabile cu securitatea cibernetică şi cu sarcinile de supraveghere şi asigurare a respectării măsurilor pentru un nivel comun ridicat de securitate cibernetică**, în scopul schimbului de informaţii privind:
  - riscurile de securitate cibernetică
  - ameninţările cibernetice şi incidentele cibernetice şi
  - riscurile, ameninţările şi incidentele noncibernetice

**Autorităţile competente sectorial (ACS), aprobate prin Decizia prim-ministrului** (cf.art.26 alin.(2) lit.b, coroborat cu art.1 alin.(4))

- elaborează **lista serviciilor esenţiale** (v. art.5), **până la 17 ianuarie 2026**, pe sectoare, astfel cum sunt delimitate la art.2 pct.3 şi pct.4 din ***Regulamentul Delegat (UE) 2023/2450 al Comisiei din 25 iulie 2023 de completare a Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului*** (v. pct.3 şi pct.4 din ***Anexa*** la **Legea 294/2024**)
  - **sectorul bancar**: (i) atragerea de depozite (instituţiile de credit); (ii) creditare (instituţiile de credit)
  - **sectorul infrastructurilor pieţelor financiare**: (i) operarea unui loc de tranzacţionare (operatorii de locuri de tranzacţionare); (ii) operarea sistemelor de compensare (contrapărţile centrale)
- **identifică entităţile critice**, **până la 17 iulie 2026**, analizând şi dacă:
  - **entitatea furnizează unul sau mai multe servicii esenţiale**;
  - **entitatea operează, iar infrastructura sa critică este situată pe teritoriul naţional şi poate include infrastructura critică naţională**, astfel cum este definită la art. 3 lit. a) din Ordonanţa de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, cu modificările şi completările ulterioare;
  - **un incident ar avea efecte perturbatoare semnificative**, determinate în conformitate cu art. 7 alin. (1), asupra furnizării de către o entitate a unuia sau mai multor servicii esenţiale ori asupra furnizării altor servicii esenţiale în sectoarele prevăzute în anexă care depind de acel serviciu esenţial sau de acele servicii esenţiale.

**Banca Naţională a României**

**Ministerul Finanţelor**

**- art.9 alin.(13) -**

**Autoritatea de Supraveghere Financiară**

- **Sectorul infrastructura digitală** (v. pct.8 din ***Anexa*** la **Legea 294/2024**)
  - - Furnizorii de internet exchange points în sensul definiţiei de la art. 6 pct. 18 din Directiva (UE) 2022/2.555 (NIS 2)
  - - Furnizorii de servicii DNS în sensul definiţiei de la art. 3 lit. d) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare, cu excepţia operatorilor de servere de nume primare
  - - Furnizorii de registre de nume de domenii de prim nivel în sensul definiţiei de la art. 6 pct. 21 din Directiva NIS2
  - - Furnizorii de servicii de cloud computing în sensul definiţiei de la art. 6 pct. 30 din Directiva NIS2
  - - Furnizorii de servicii de centre de date în sensul definiţiei de la art. 6 pct. 31 din Directiva NIS2
  - - Furnizorii de reţele de furnizare de conţinut în sensul definiţiei de la art. 6 pct. 32 din Directiva NIS2
  - - Prestatorii de servicii de încredere în sensul definiţiei de la art. 3 pct. 19 din Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE
  - - Furnizorii de reţele publice de comunicaţii electronice în sensul definiţiei de la art. 4 alin. (1) pct. 6 din OUG nr.111/2011 privind comunicaţiile electronice, aprobată cu modificări şi completări prin Legea nr. 140/2012, cu modificările şi completările ulterioare
  - - Furnizorii de servicii de comunicaţii electronice în sensul definiţiei de la art. 4 alin. (1) pct. 9 din OUG nr.111/2011, aprobată cu modificări şi completări prin Legea nr. 140/2012, cu modificările şi completările ulterioare, în măsura în care serviciile acestora sunt destinate publicului

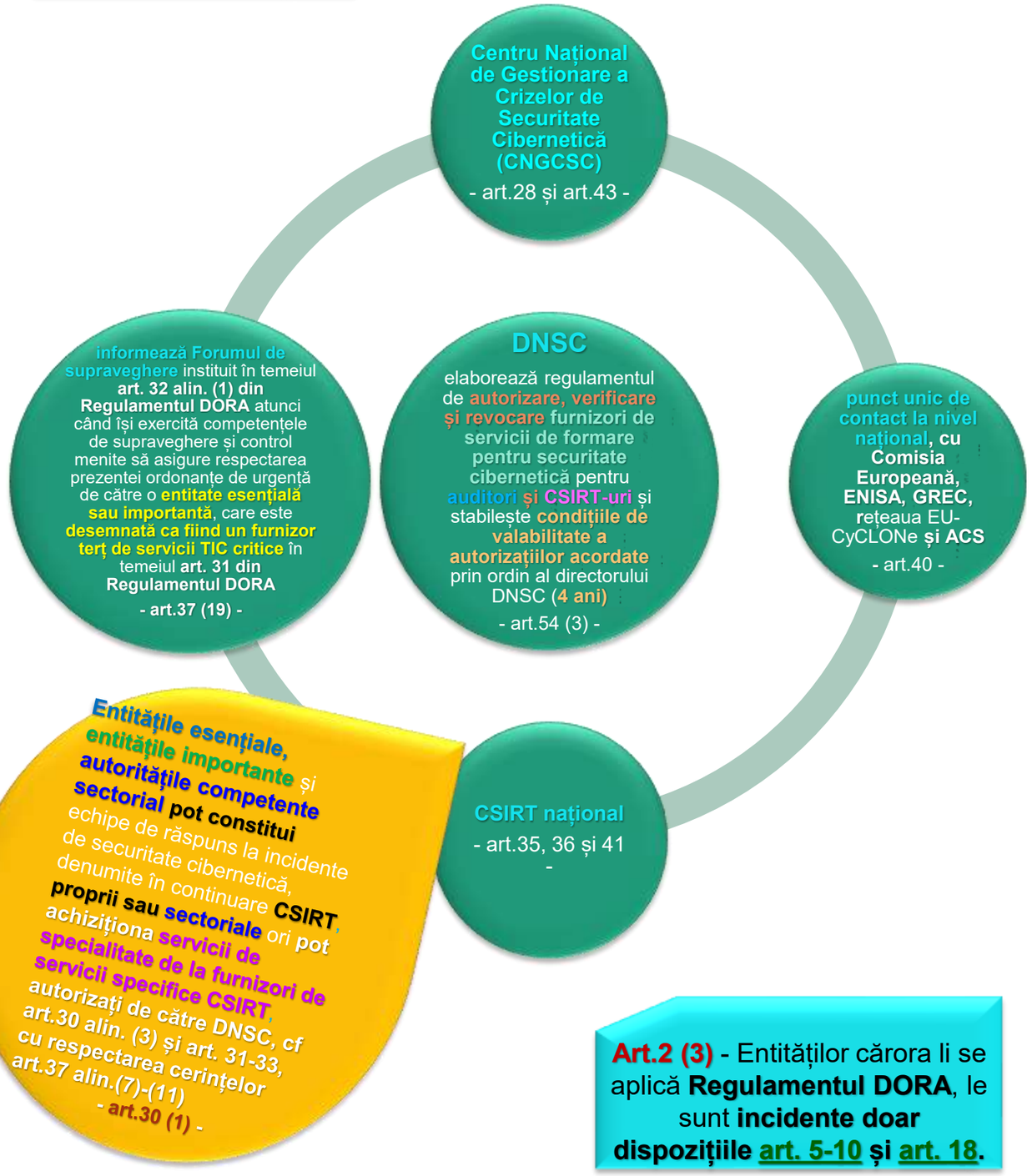
**Autorităţile competente responsabile cu securitatea cibernetică - DNSC**
- art.9 alin.(14) -

**Centrul Naţional pentru Coordonare și Protecția Infrastructurilor Critice (CNCPIC)**
- art.9 alin.(15) -

**informează Comisia Europeană** cu privire la **desemnarea unei alte autorităţi** decât autorităţile competente menţionate la alin. (13) şi (14) drept autoritate competentă în ceea ce priveşte entităţile critice din sectoarele prevăzute la pct. 3, 4 şi 8 din tabelul din anexă

# GUVERNANȚA DE SECURITATE CIBERNETICĂ
# LA NIVEL NAȚIONAL

**OUG nr.155/2024**




**Art.2 (3)** - Entităților cărora li se aplică **Regulamentul DORA**, le sunt **incidente doar dispozițiile art. 5-10 și art. 18.**

**DNSC se consultă și cooperează cu**:

- **ANCOM**, pentru **sectorul „8**. Infrastructură digitală“: „***Furnizorii de IXP*** (internet exchange point)“, „***Furnizorii de servicii de centre de date***“, „***Furnizorii de rețele publice de comunicații electronice***“ și „**Furnizorii de servicii de comunicații electronice destinate publicului**“ din anexa nr. 1 și pentru **sectorul „1**. ***Servicii poștale și de curierat***“ din anexa nr. 2;
- **autoritățile competente responsabile cu energia electrică și cu securitatea cibernetică**, definite cf. *Regulamentului delegat (UE) 2024/1366 de completare a Regulamentului (UE) 2019/943 prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de* ***securitatea cibernetică a fluxurilor transfrontaliere de energie electrică***
- **Autoritatea pentru Digitalizarea României (ADR)**, pentru **sectorul „8**. Infrastructură digitală“: „***Prestatorii de servicii de încredere***“ și în domeniul transformării digitale și societății informaționale
- **autorități competente sectorial** în domeniul securității cibernetice, conform anexelor nr. 1 și 2, **desemnate de către ministerele de resort**, prin hotărâre a Guvernului
- **CNCPIC**, identificarea entităților esențiale/ critice
- **Banca Națională a României (BNR)** și **Autoritatea de Supraveghere Financiară (ASF)**, pentru evaluarea și gestionarea riscurilor cibernetice, identificarea vulnerabilităților și implementarea măsurilor de protecție adecvate **entităților esențiale** și **entităților importante** din **domeniul bancar** și al **infrastructurilor pieței financiare**, sens în care:
  - **a) BNR** și **ASF transmit** în timp util către DNSC **informații privind incidentele majore** legate de TIC și **amenințările cibernetice semnificative**, raportate de către entitățile cărora li se aplică cerințele Regulamentului DORA, iar **DNSC transmite** către **BNR** și **ASF informații privind incidentele majore și amenințările cibernetice, raportate de către entitățile esențiale sau importante cărora li se aplică OUG 155/2024 și care au fost desemnate conform Regulamentului DORA drept furnizori terți esențiali de servicii TIC**;
  - **b) BNR** și **ASF pot solicita** orice tip de **consultanță și asistență tehnică** relevantă din partea DNSC, în limita capacităților și resurselor DNSC, și **pot stabili acorduri de cooperare** pentru a permite crearea unor mecanisme de coordonare eficace și rapide
- **Autoritatea Aeronautică Civilă Română (AACR)**, pentru evaluarea și gestionarea riscurilor cibernetice, identificarea vulnerabilităților și implementarea măsurilor de protecție adecvate **entităților din domeniul transporturilor aeriene**
- **Serviciul Român de Informații** (securitate națională)
- **Ministerul Apărării Naționale** (apărare națională)
- **Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază** (servicii esențiale în domeniul lor de activitate și responsabilitate)
- **organele de urmărire penală**
- **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, **în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii**.

# GUVERNANȚA DE SECURITATE CIBERNETICĂ
# LA NIVELUL ECOSISTEMULUI FINANCIAR-BANCAR ÎN ROMÂNIA

**Autoritățile Competente Sectorial (ACS)**

Legea 294/2024

OUG 155/2024

**Banca Națională a României**

**Ministerul Finanțelor**

- art.9 alin.(13) -

**Centrul Național de Coordonare pentru Protecția Infrastructurilor Critice (CNCPIC)**

OUG 98/2010

**Directoratul Național de Securitate Cibernetică (DNSC) - OUG. 104/2021**

Autoritățile pot adopta o **abordare bazată pe risc** pentru **a prioritiza sarcinile de supraveghere**

elaborează **lista serviciilor esențiale** (v. art.5), **până la 17 ianuarie 2026**, pe sectoare, astfel cum sunt delimitate la art.2 pct.3 și pct.4 din ***Regulamentul Delegat (UE) 2023/2450 al Comisiei din 25 iulie 2023 de completare a Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului*** (v. pct.3 și pct.4 din ***Anexa*** la **Legea 294/2024**)

- **sectorul bancar**: (i) atragerea de depozite (instituțiile de credit); (ii) creditare (instituțiile de credit)
- **sectorul infrastructurilor piețelor financiare**: (i) operarea unui loc de tranzacționare (operatorii de locuri de tranzacționare); (ii) operarea sistemelor de compensare (contrapărțile centrale)

**identifică entitățile critice**, **până la 17 iulie 2026**, analizând și dacă:

- **entitatea furnizează unul sau mai multe servicii esenţiale**;
- **entitatea operează, iar infrastructura sa critică este situată pe teritoriul naţional şi poate include infrastructura critică naţională**, astfel cum este definită la art. 3 lit. a) din Ordonanţa de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, cu modificările şi completările ulterioare;
- **un incident ar avea efecte perturbatoare semnificative**, determinate în conformitate cu art. 7 alin. (1), asupra furnizării de către o entitate a unuia sau mai multor servicii esenţiale ori asupra furnizării altor servicii esenţiale în sectoarele prevăzute în anexă care depind de acel serviciu esenţial sau de acele servicii esenţiale.

**« principiul de *"Chinese wall"* PROTOCOL funcția de *"operator servicii esențiale "»***

**Operatorii de Servicii Esenţiale (OSE)**

**persoană fizică** sau **juridică de drept public sau privat** de tipul celor prevăzute în **anexa la Legea 362/2018**, care furnizează un **serviciu** considerat **esenţial** conform legii

**Serviciul** este considerat **esenţial** dacă:

- este utilizat în susținerea unor activități sociale și / sau economice de cea mai mare importanță;
- furnizarea sa depinde de o rețea sau de un sistem informatic; și
- furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident.

**DNSC**

**SOC / CSIRT interne**

**furnizorul de servicii de securitate gestionate** (Managed Security Services Provider - MSSP) **cf.def. – art.6(40)**

**Centre de operațiuni de securitate (SOC)**

VS.

**Echipe de răspuns la incidente de securitate informatică (CSIRT)**

**Art.30-35 din OUG 155/2024**

raportare / răspuns la incidente

- **Măsuri minime de securitate pentru operatorii de servicii esențiale**

• *Sursa: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services)*

ISO 27001
NIST CSF
ISA/IEC 62443

- **ORDIN SGG nr. 1.323 din 9 noiembrie 2020** pentru aprobarea ***Normelor tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale***

**Publicat în: Monitorul Oficial nr.1.142 din 26 noiembrie 2020**

***"Guvernanță anticipativă"***

**Chief Information Security Officer (CISO)** | **Chief Risk Officer (CRO)** | **Ofițer de legătură pentru securitate ICN/ ICE (OLS)** | **Data Protection Officer (DPO)** | **Responsabil SITU/SSM**

**Registru de informații** în legătură cu **toate acordurile contractuale** privind **utilizarea serviciilor TIC oferite de furnizori terți de servicii TIC necritici și critici - art.28(3) și (9) din DORA**

**Conducere structuri organizatorice digitalizate / care oferă produse sau servicii**
(high și middle management)
- reducere muncă repetitivă/redundantă
- minimizare risc erori umane
- concentrare pe sarcini mai importante

**MANAGEMENT RISC INTEGRAT**


# GUVERNANȚA DE SECURITATE CIBERNETICĂ LA NIVELUL PIEȚELOR FINANCIARE ÎN ROMÂNIA

14.08.2024

”*Regulamentul DORA va spori încrederea investitorilor în piețele financiare*”

Alexandru Petrescu, președintele ASF

Sursa: *https://studiifinanciare.ro/presedintele-asf-regulamentul-dora-va-spori-increderea-investitorilor-in-pietele-financiare*


**Plan transpunere directive**

- **Transpunerea în legislația națională a Directivei corespunzătoare - 2022/2556** a Parlamentului European și a Consiliului din 14 decembrie 2022 de modificare a Directivelor 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 și (UE) 2016/ 2341 **în ceea ce privește reziliența operațională digitală pentru sectorul financiar**

**LEGE nr.306 din 05.12.2024**
**modifică**
**Lege 126/2018**
**OUG 32/2012**
**Lege 297/2004**
**Lege 74/2015**

**Decizii desemnare:**

- **autorități competente** din România, responsabile cu **asigurarea conformității**
- **entități de supraveghere** conform DORA și definire **competențe de supraveghere și de executare**
- **autoritate competentă** în ceea ce privește **securitatea rețelelor și a informațiilor pentru instituțiile de credit și infrastructurile pieței financiare** care au fost **identificate ca Operatori de Servicii Esențiale** („OES”), precum **și pentru Furnizorii de servicii digitale** („FSD”) **care sunt deja sub supravegherea DNSC („autoritatea NIS”)** ”(...) pentru ***a asigura cooperarea transfrontalieră cu alte state membre și cu Grupul de cooperare*** pentru rețele și sisteme informatice” (v. *Recomandarea Comitetului European pentru Risc Sistemic (CERS/2021/17) din 02.12.2021 privind un cadru pan-european de coordonare sistemică a incidentelor cibernetice pentru autoritățile relevante*)

**Aplicare Regulament DORA**

- **caracter executoriu – 17 ianuarie 2025**
- **entităților financiare** care intră sub incidența sa (v. **art.2**)

**LEGE 294/2024**
**Și**
**OUG 155/2024**

# GUVERNANȚA DE SECURITATE CIBERNETICĂ
# LA NIVELUL FINTECH / ”*LANȚULUI DE APROVIZIONARE*” ÎN ROMÂNIA

***Legea nr.58/2023 privind securitatea și apărarea cibernetică a României***

***Strategia de securitate cibernetică a României, pentru perioada 2022—2027***, adoptată prin HG nr.1321 din 30.12.2021

susțin securitatea și apărarea cibernetică națională

***nu au un ”ecou” pe măsura intensității cu care s-au propagat***

***nu sunt*** **subscrise** ”***direcțiilor de dezvoltare și investiții în domeniul securității cibernetice***”

**inovațiile și resursele financiare investite de sectorul privat românesc – reale ”infuzii”**

**drepturile de proprietate intelectuală**

care se propun ***Consiliului Suprem de Apărare a Țării*** de către ***Consiliul Operativ de Securitate Cibernetică (COSC)***, în aplicarea art.9 alin.(1) lit.e) din *Legea nr.58/2023 privind securitatea și apărarea cibernetică a României*

**parteneriatele public-privat**

***- benefice***
***- indispensabile***

***- la nivelul sectorului financiar-bancar***
***- la nivel național***

**crearea unui ecosistem de securitate rezilient și adaptabil**


**Mediul de afaceri**

**nu mai poate fi considerat un actor pasiv în ceea ce privește contribuția și chiar apartenența sa la asigurarea securității naționale**

***pregnant prezent*** pe **piața financiară**

***intens implicat*** în **colaborarea cu autoritățile naționale** cu competență

Pe fondul politic și economic turbulent, **din 2024**, **industria financiară din România a crescut cheltuielile IT cu 7,6%**

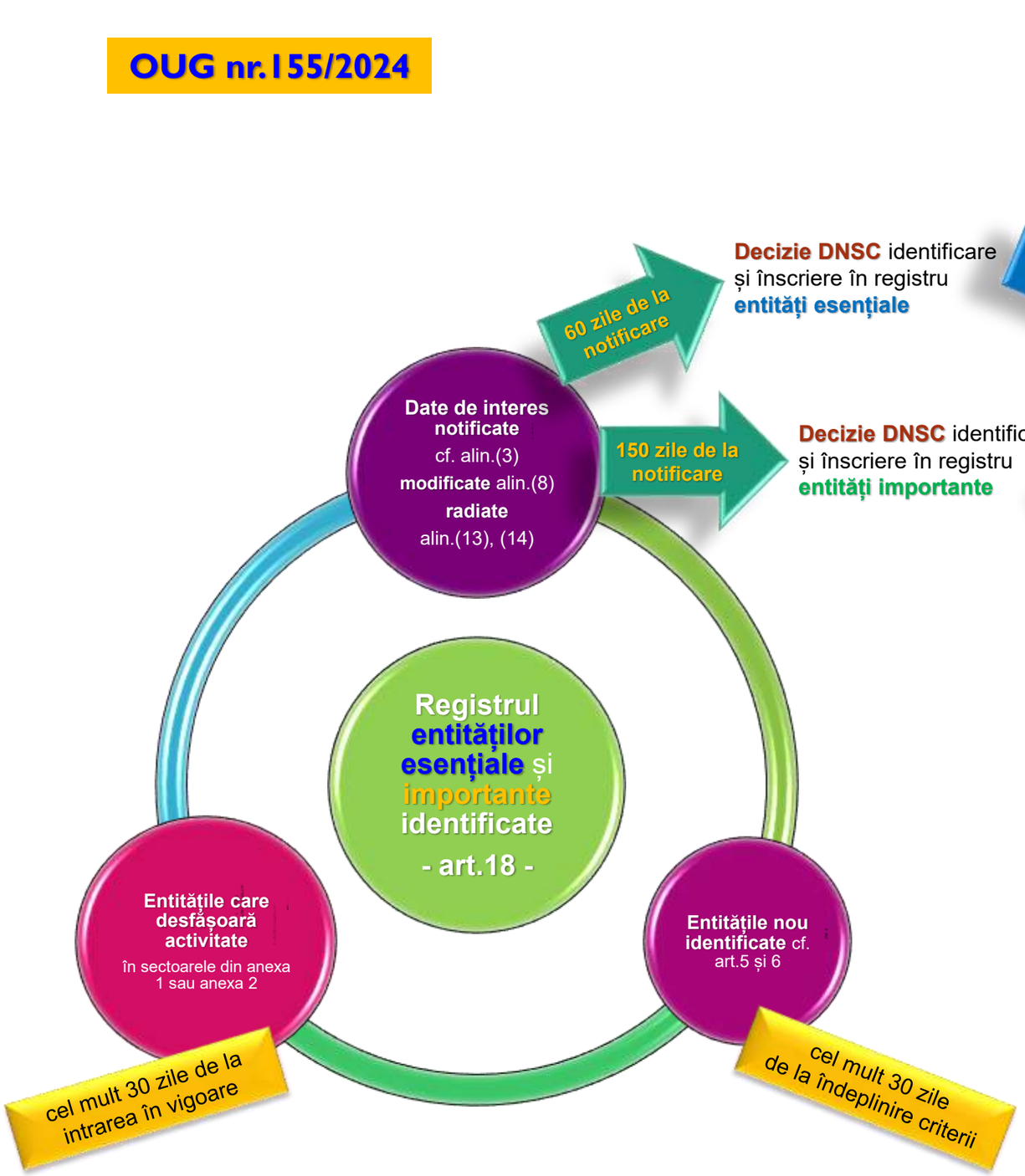
- ***software*** (19,6%)
- ***Business Services*** (6,1%)
- ***IT Services*** (5,9%), indicând astfel o concentrare deosebită pe ***proiecte de digitalizare, inovație, securitate și eficiență operațională***

Sursa: IDC WW ICT Spending Guide 2024

- ***programe de conștientizare publică***
- ***activități de creștere a nivelului de cultură de securitate cibernetică***
- ***promovare a unor măsuri de igienă în spațiul cibernetic*** etc.

# GUVERNANȚA DE SECURITATE CIBERNETICĂ
# LA NIVELUL FINTECH / "*LANȚULUI DE APROVIZIONARE*" ÎN ROMÂNIA

**OUG nr.155/2024**




**Decizie DNSC** identificare și înscriere în registru **entități esențiale**

60 zile de la comunicare

**Decizie DNSC** identificare și înscriere în registru **entități importante**

60 zile de la comunicare

**transmit DNSC evaluarea nivelului de risc** al entității cf. art.10 alin.(2)

60 zile de la evaluare

autorități competente sectorial (ACS)

anual

**plan de măsuri** pentru remedierea deficiențelor identificate, asumat de managementul entității, în conformitate cu măsurile de gestionare a riscurilor aplicabile acestora

realizează **autoevaluare a nivelului de maturitate** a măsurilor de gestionare a riscurilor de securitate cibernetică cf. art.12 alin.(4), pe baza:

- 17 ian. 2025 modificări / 2 ani
- 17 aprilie 2025

**Ordin DNSC nr.1/2025 și Ordin DNSC nr.2/2025** privind măsurile de gestionare a riscurilor prevăzute la art. 11 alin. (1) în ceea ce privește **cerințele tehnice, operaționale și organizatorice**, conform art. 13

**PROTOCOL**

**notificare ENISA** **date de interes** cf. alin.(10)

**notificare Comisia Europeană** denumiri **entități esențiale** și **entități importante identificate în baza art. 9**

**informare autorități competente sectorial (ACS)** cf. alin.(18)

**ordinele comune, DNSC / ACS**, în domeniul securității cibernetice din domeniul de competență, **în vederea asigurării unui nivel comun ridicat de securitate cibernetică la nivel național, inclusiv** în ceea ce privește **măsurile** tehnice, operaționale și organizatorice de gestionare a riscurilor, proporționale și adecvate **pe care entitățile din domeniul de competență au obligația de a le lua** în desfășurarea activității lor, **procedura de notificare și de răspuns la incidentele de securitate cibernetică** aplicabile entităților din domeniul de competență, **pragurile specifice și criteriile de stabilire a impactului incidentelor de securitate din domeniul de competență**

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ

«(...țările) **”să își construiască reziliență**”, pentru că „***în absența unor bariere de siguranță suficiente, am putea ajunge la o fragmentare severă a economiei globale și, în consecință, la o productivitate și un nivel de venit mai scăzute pentru toată lumea***”.»

*Gita Gopinath, prim-director general adjunct al Fondului Monetar Internațional - Discurs din **iunie 2024**, preluat în raportul World Economic Forum din **ianuarie 2025***

**Obiectiv major:**
**combaterea riscului cibernetic concentrat în lumea noastră interconectată**

- afectată **economia globală**
- subestimată **securitatea națională** a fiecărui stat
- amenințată **infrastructura** (tehnologia operațională) **critică** pentru afaceri

**Securitatea cibernetică**
**- amenințări majore -**

**rezilienţa societală**

- **capacitatea de a rezista în faţa provocărilor şi de a le face faţă**
  - **Protejarea infrastructurii** – protecția rețelelor energetice, financiare și de comunicații
- **a realiza tranziţii într-un mod durabil, echitabil şi democratic**
  - **Legislație și politici publice** – actualizarea constantă a legislației pentru
- **UE şi TM să facă faţă unor crize mai complexe, trans-sectoriale şi trans-frontaliere**
  - **Capacități de răspuns** – consolidarea echipelor CERT cu resurse și tehnologie avansată
- **gestionarea evenimentelor, în raport cu riscurile cunoscute, prefigurate sau neașteptate**
  - **Educația** – pregătire continuă, diferențiat, pe grupuri-țintă, în funcție de nivelul de decizie etc.

**rezilienţa operaţională**

Mijloace:
- **gândirea conceptuală pragmatică** și realizarea practică a ”*planului abstracţiei logice*” (**obiecte, fenomene sau procese** – **IF / THEN / ELSE** – **scenarii și ipoteze**) / **roluri / responsabilități**
- atenția și efortul pentru **a diminua**, **a atenua** și **a contracara terorismul cibernetic**
- **acțiuni** comune, unitare, bine organizate și coordonate **(pe plan intern / internațional)**


# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ

*„Conformitatea este capacitatea de a demonstra unei terțe părți că ai pus în aplicare procesele pentru a fi rezistent”*

***Dean Carter, Managing Director al SafeAdvisory***


**Cerințe uniforme de securitate cibernetică** pentru proiectarea, dezvoltarea și producția **produselor digitale** (laptopuri, smartphone-uri, dispozitive pentru casă inteligentă și sisteme industriale)

**Marcajul CE pentru conformitatea cu securitatea cibernetică** (**r**espectă standardele UE de siguranță, sănătate și protecție a mediului**)**

**se aplică tuturor produselor conectate la o rețea sau la un alt dispozitiv – direct sau indirect** (cu excepția **dispozitivelor medicale**, **produselor aeronautice** și **autovehiculelor**)

îmbunătățește transparența și oferă consumatorilor posibilitatea de a lua decizii informate în ceea ce privește **caracteristicile de securitate cibernetică ale produselor digitale**

**„*Actul privind reziliența cibernetică*” (CRA) - Regulamentul (UE) 2024/2847 privind cerințele de securitate cibernetică pentru produsele cu elemente digitale (inclusiv software și hardware) și de modificare a Regulamentului (UE) 2019/1020**

**în vigoare la 10.12.2024 / aplicat de la 11.12.2027**

**complementează NIS2 și DORA**

- **standardizare**
- **măsuri unitare**

- **reguli achiziție produse cu elemente digitale, pentru a garanta securitatea cibernetică**
- **cerințe de proiectare, dezvoltare și producție a acestor produse**
- **cerințe esențiale pentru procesele de management al vulnerabilităților instituite de producători**
- **supravegherea pieței digitale și aplicarea legii**

- **Conformitatea securității** și **reziliența cibernetică** sunt **concepte distincte, dar interconectate**, care joacă un **rol crucial în protejarea organizațiilor de amenințările cibernetice**
- **Conformitatea (legalitatea)** servește ca **fundație pentru construirea încrederii** cu părțile interesate, în timp ce **reziliența cibernetică** se concentrează pe **capacitatea de a recupera pierderile / restabili continuitatea rapid, în cazul unui incident**


**set echilibrat de măsuri**

**obligații de reglementare** și **răspuns proactiv la incidente**

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ


**Digitalizarea**

- **servicii la distanţă**
- **soluţii inovative**

## Centrele de date / Fintech-urile *(ne)conforme ?*

***Centrul de date hyperscale deținut de Google în Council Bluffs, Iowa, SUA***

**2023**
Aprox. 6,7 zettabytes (ZB) de date stocate online

**2025**
Cca 16 zettabytes (ZB) de date stocate online

**Inteligența artificială (AI)**

- creșterea inovației și integrării în **industrie** pentru a susține **procesarea de înaltă densitate**
- atenție sporită acordată **reglementărilor legate de AI**
- accent tot mai mare pe **sustenabilitate** și eforturi de **securitate cibernetică**

**2026** Cerere globală de electricitate - peste 80% .

**2030** Cerere globală de electricitate - peste 160%

| Avantaje | Provocări |
|---|---|
| Noi produse/servicii | Modificările profunde în cererile clienților |
| Fluxuri de informații și cunoștințe | Uzura morală rapidă a produselor online |
| Tehnologii digitale | Modificările majore în **abilitățile necesare resurselor umane** |
| Interconectivitate digitală | **Convergența mai multor tehnologii** |
| Acces facil la clienți și piețe cu potențial | **Aspectele legate de securitatea cibernetică** |

- Care este tipul de cloud?
- Cine are acces la date?
- Unde sunt datele?
- Datele sunt salvate?
- Care este structura de control a terților?
- Puteți efectua due diligence eficient/continuu?
- Cât de dificil este să te deconectezi?

**Dacă un furnizor nu vă spune unde sunt stocate datele, găsiți un alt furnizor**

**Centre de date în România – 59** medii și mari și alte peste 100 de dimensiuni mai mici.
Exemple:

- **București** (27) - zona Preciziei (4 hectare)
  - cartierul Vitan (27.734 mp - **Portland Trust**, dezvoltator imobiliar)
  - Infinity Cloud Technologies, cu sediul în Dubai (1200 mp)
  - Google (intenție)
- **Craiova** (5) - ClusterPower
- **Timișoara** (9)
- **Brașov** (4)
- **Cluj-Napoca** (8)


# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ

## Tendințe în centrele de date

**Infrastructura de alimentare și răcire inovează pentru a ține pasul cu densificarea procesării**

- **Rack-urile AI vor necesita sisteme UPS** (baterii, echipamente de distribuție a energiei și aparataj de comutare cu **densități mai mari de putere**)
- **Sistemele de răcire hibridă,** cu configurații **lichid-lichid**, **lichid-aer** și **lichid-refrigerant**
- **Sistemele de răcire cu lichid** vor fi din ce în ce mai des asociate cu propriile lor sisteme UPS de înaltă densitate **pentru a asigura funcționarea continuă**
- **Serverele vor fi integrate** tot mai mult **cu infrastructura necesară pentru a le susține**

**Centrele de date prioritizează provocările privind disponibilitatea energiei**

- **Reglementarea centrelor de date**, inclusiv a potențialelor **restricții asupra modului de construcție** a lor și **a utilizării energiei la nivelul acestora**
- **Alimentarea microrețelelor** cu **celulele de combustibil** și **combinații chimice alternative** pentru baterii
- **Dezvoltarea de reactoare modulare mici** pentru centrele de date și alți consumatori mari de energie

**Jucătorii din industrie colaborează pentru dezvoltarea fabricilor de AI**

- **Planuri strategice transparente pentru adoptarea AI** între **dezvoltatorii de cipuri, clienții, producătorii de infrastructură de alimentare și răcire, utilitățile și alți actori din industrie**
- **Instrumente de dezvoltare alimentate de AI** pentru a accelera **ingineria** și **fabricarea designurilor standardizate și personalizate**
- **Parteneriate de producție** care permit **integrarea reală a IT-ului și infrastructurii**

**AI face ca securitatea cibernetică să fie mai dificilă - dar și mai ușoară**

- **Analiza mai largă a proceselor de securitate cibernetică și a rolului pe care comunitatea centrelor de date îl joacă** în **prevenirea atacurilor de tip ransomware**
- **Respectarea acelorași cerințe de securitate și de componente ale rețelei**, pentru ca **centrele de date să nu poată deveni inutilizabile** - atacurile încep tot mai des cu un **hack susținut de AI asupra sistemelor de control, dispozitivelor integrate sau sistemelor de infrastructură conectate**
- **Dezvoltarea de tehnologii proprii sofisticate de securitate AI,** în timp ce **fundamentele și cele mai bune practici de apărare în profunzime și diligență extremă rămân aceleași**, însă, **natura, sursa și frecvența atacurilor se modifică**

**Guvernele și reglementatorii din industrie abordează aplicațiile AI și utilizarea energiei**

- **Evaluarea implicațiilor AI și dezvoltarea normelor** pentru utilizarea acesteia
- **Inaugurarea propriilor supercomputere AI** suverane, iar multe alte țări vor iniția **propriile proiecte de AI suverană și procese legislative** pentru a dezvolta cadre de reglementare proprii

**Directiva UE 1791/2023 privind eficiența energetică**
**(înlocuiește Directiva 2012/27/UE)**
https://sintact.ro/legislatie/jurnalul-oficial-ue/directiva-1791-13-sept-2023-privind-eficienta-energetica-si-de-79173987

**Cerințe detaliate** de raportare:
- ❑ nivel de consum
- ❑ estimări de eficientă energetică (PUE)
- ❑ metode de reutilizare a căldurii generate

**18 nov. 2024**
Ministerul Energiei a lansat în dezbatere publică proiectul de Ordonanța de urgență

**3 febr. 2025**
Proiect OUG de modificare a **Legii nr. 121/2014 privind eficiența energetică**

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ


**3 aprilie 2025**

## Investiții CEO

- 72% vor investi în 2025, față de 40% în 2024
- 68% cred că GenAI va avea cel mai mare impact asupra productivității angajaților și 35% se așteaptă să înceapă să vadă rentabilitatea investiției de la GenAI în decurs de șase luni
- 67% au remarcat că folosesc personal GenAI cel mai mult pentru investiții sau cercetare de piață

**GenAI**


- 71% dintre firme fac investiții majore în blockchain și tehnologii de registru distribuit (DLT) în 2025, față de 59% în 2024
- 64% fac investiții mari în criptomonede, în creștere de la 51% în 2024
- 47% consideră că DLT permite dezvoltarea de noi oportunități în ecosistemul piețelor de capital
- 73% sunt de acord că vor exista reglementări și guvernanță mai mari în ceea ce privește activele digitale în viitor

**Active digitale**

- 86% dintre firme îl integrează în procesele lor, iar 84% fac investiții moderate spre mari în 2025
- 31% au selectat platforme și aplicații cloud, iar 27% plănuiesc să-și mărească investiția în tehnologie în următorii doi ani

**Cloud**

**Instituția financiară este responsabilă pentru orice încălcare a conformității din partea furnizorilor terți**

***Studiu anual de transformare digitală și tehnologie de nouă generație***

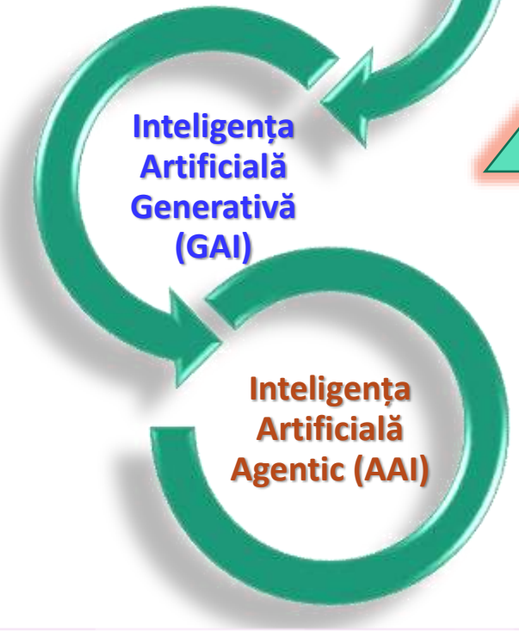
*Sursa: **Broadridge Financial Solutions**, https://www.broadridge.com/de/press-release/2025/ai-and-digital-asset-investments-rise-per-broadridge-study*

***Investițiile în inteligența artificială și activele digitale cresc în timp ce provocările tehnologice vechi și compromiterea datelor persistă***

***Amenințarea de fraudă generată de Inteligența Artificială Generativă (GAI)***
**- Raport UK National Crime Agency -**

**Tipuri de fraudă generate cu GAI:**

| | |
|---|---|
| **Furtul de identitate** | • uzurpare identitate directori / salariați |
| **Deep-fake** | • creare identități sintetice |
| **Inginerie socială** | • phishing avansat prin e-mail<br>• Spoofing, vishing etc. |
| **Falsificarea documentelor (pașapoarte, permise de conducere, cărți naționale de identitate, certificate de naștere)** | • **Contrafacere fizică**: un document fizic fals creat de la zero<br>• **Contrafacere digitală**: o reprezentare digitală falsă a unui document creat de la zero (adică, în Photoshop)<br>• **Fals fizic**: un document existent care este modificat sau editat<br>• **Fals digital**: un document existent care este modificat sau editat folosind instrumente digitale |
| **Generare conținut fraudulos (în lanțurile de aprovizionare)** | • creare **profiluri false** în rețelele sociale, **recenzii false** sau **conținut de marketing înșelător**, adesea menit să submineze încrederea sau să manipuleze percepțiile<br>• creare de **documente și contracte realiste** |




- ❑ **Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul AI)**
- ❑ **Ghidurile de etică pentru inteligența artificială de încredere**
- ❑ **Lista de evaluare a inteligenței artificiale de încredere (ALTAI)**

**27 mai 2024**

**- la nivel național -**

:**Propunerea legislativă** privind AI
(PLx 336/27.05.2024)
- **trimisă pentru raport la comisiile permanente ale Camerei Deputatilor (după respingerea de către Senat)**
- **avizată de Comisia pentru apărare, ordine publică şi siguranţă naţională, la 18.06.2024, Comisia juridică, de disciplină şi imunităţi, la 05.03.2025 și Comisia pentru tehnologia informaţiei şi comunicaţiilor, la 06.03.2025**
- **respinsă de Comisia pentru știință și tehnologie, la 15.04.2025**

**Ministerul Cercetării, Inovării și Digitalizării** a supus aprobării Guvernului României:
- **HG nr. 832/11.07.2024** privind **aprobarea Strategiei Naționale pentru Inteligența Artificială 2024-2027**
- **HG nr.1028/21.08.2024** privind **aprobarea Strategiei naționale în domeniul tehnologiilor cuantice pentru perioada 2024-2029**

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ

**Continuitatea afacerii vs. Managementul riscului integrat (sub raport procedural, tehnic și organizatoric)**

**Reziliența afacerii** = **capacitatea unei organizații** de **a anticipa**, de **a se pregăti** și de **a se adapta la condițiile în schimbare** și de **a rezista** și de **a se recupera rapid după întreruperi (** ex. **întreruperi de curent, breșe de date și defecțiuni ale sistemului**)

**Evaluarea riscurilor (de) pe rețelele de socializare**

**18 mai 2023**

**SUA**

utilizare pentru **marketing și profit**

identificare **riscuri asociate** privind **conformitatea legală și de reglementare**

monitorizare pentru **comentarii negative și plângeri**

**educare angajați cu privire la modul de utilizare a rețelelor sociale**

- **politici și proceduri utilizare oficială și personală**, inclusiv **definirea activităților nepermise**
- **protejarea informațiilor nepublice și asigurarea acurateței/imparțialității celor comunicate** (ex. distribuire conținut controversat pe conturile sale de socializare / către prieteni)

**martie 2023**


- **banca falimentată** (**10 ore - 42 de miliarde de dolari**)
- ***creditorul*** a anunțat că **vinde titluri de valoare** și strânge capital
- clienții ”nervoși” au retras **1 milion de dolari / secundă**

**Business Continuity Planning (BCP) devine Business Continuity Management (BCM)**

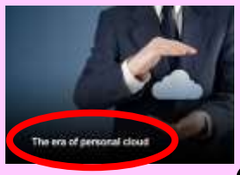
- înseamnă să ai un **plan de redresare și reluare a operațiunilor după o întrerupere neașteptată**
- acoperă **scenarii pentru orice eventualitate**, asigurându-se că un FI este pregătit **să răspundă la o întrerupere sau la un eveniment**

**BCP**


- procesul prin care **managementul instituției supraveghează și implementează capacitățile de rezistență, continuitate și răspuns** pentru **a proteja angajații, clienții și produsele și serviciile**
- pune accentul pe aspectul de **gestionare a riscurilor și vulnerabilităților care amenință reziliența instituției** (**acțiuni proactive**) și **împietează asigurarea continuității afacerii**

**BCM**


Psihologia socială




Cyber-psihologia

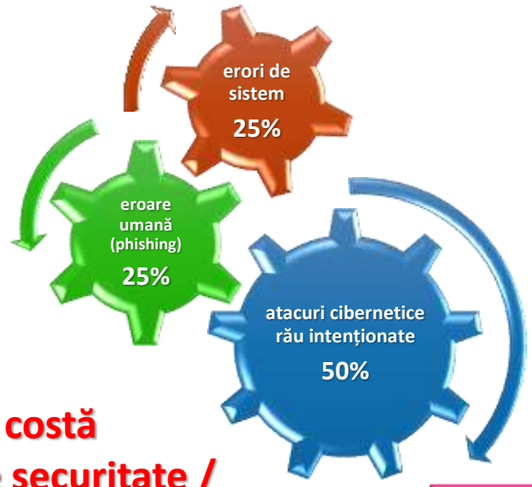


# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ

## Managementul riscului integrat (sub raport procedural, tehnic și organizatoric)

**Stabilire context – grad de afectare (severitate)** activitate comercială, proces sau proiect specific etc.

- ❑ echipa știe **ce/cum este (de) evaluat**
- ❑ **examinare rezultate** ***puncte forte, puncte slabe, oportunități și amenințări (SWOT)*** sau ***analize politice, de mediu, sociale și tehnologice (PEST)***
- ❑ **analizare raport anterior**
- ❑ stabilire existență **decalaje/ modificări** ale orientărilor/ recomandărilor aplicabile **de la ultima evaluare**




**Identificare și management integrat riscuri** (operațional, de tranzacție, de conformitate, de credit, strategic, de reputație, de terță parte, cibernetic și de concentrare)

**Analiză și evaluare:**
- **i**mpact financiar propriu / complementar
- nivel de implicare a terților
- **eșec de conformitate**

# Procesul de evaluare a riscului

**Cât costă o breșă de securitate / încălcare a datelor?**

**Cauză - Efect**
**breșe de securitate / încălcare date**

**Limitarea riscului reputațional / financiar**, prin:
- **declarare / detecție timpurie breșe**
- **managementul continuității afacerii (BCM)**
- **plan de răspuns la incidente bine testat**
- **plan recuperare în caz de dezastre (RPD)**
- **acoperirea asigurării cibernetice (instituțională / a terților)**
- **monitorizarea cibernetică a furnizorilor terți**

- ❑ **Procesele de evaluare a riscurilor nu sunt consecvente în întreaga organizație**, ceea ce duce la definiții diferite ale riscului în fiecare departament și la o expunere mai mare la risc
- ❑ **Angajații:**

**- nu reușesc să identifice riscurile potențiale pentru că se tem că se vor reflecta negativ asupra performanței lor**.

**- nu știu care sunt parametrii**

- ❑ Nu există un **proces continuu sau o verificare fiabilă** pentru a se asigura că **controalele riscurilor sunt valabile pe tot parcursul ciclului de viață al riscului.**


## Scoaterea din uz a sistemului clasificat / nepublic


- **procedural**
- **tehnic**

/ 328

- **Medii de stocare – după declasificare, prin ştergerea sigură cu mecanisme certificate**
- **Mediile pe care au fost stocate informaţii CTS / TRES SECRET UE / SSID nu pot fi reutilizate, *trebuie distruse***
- **Echipamente TEMPEST / criptate – după îndepărtarea caracteristicilor**

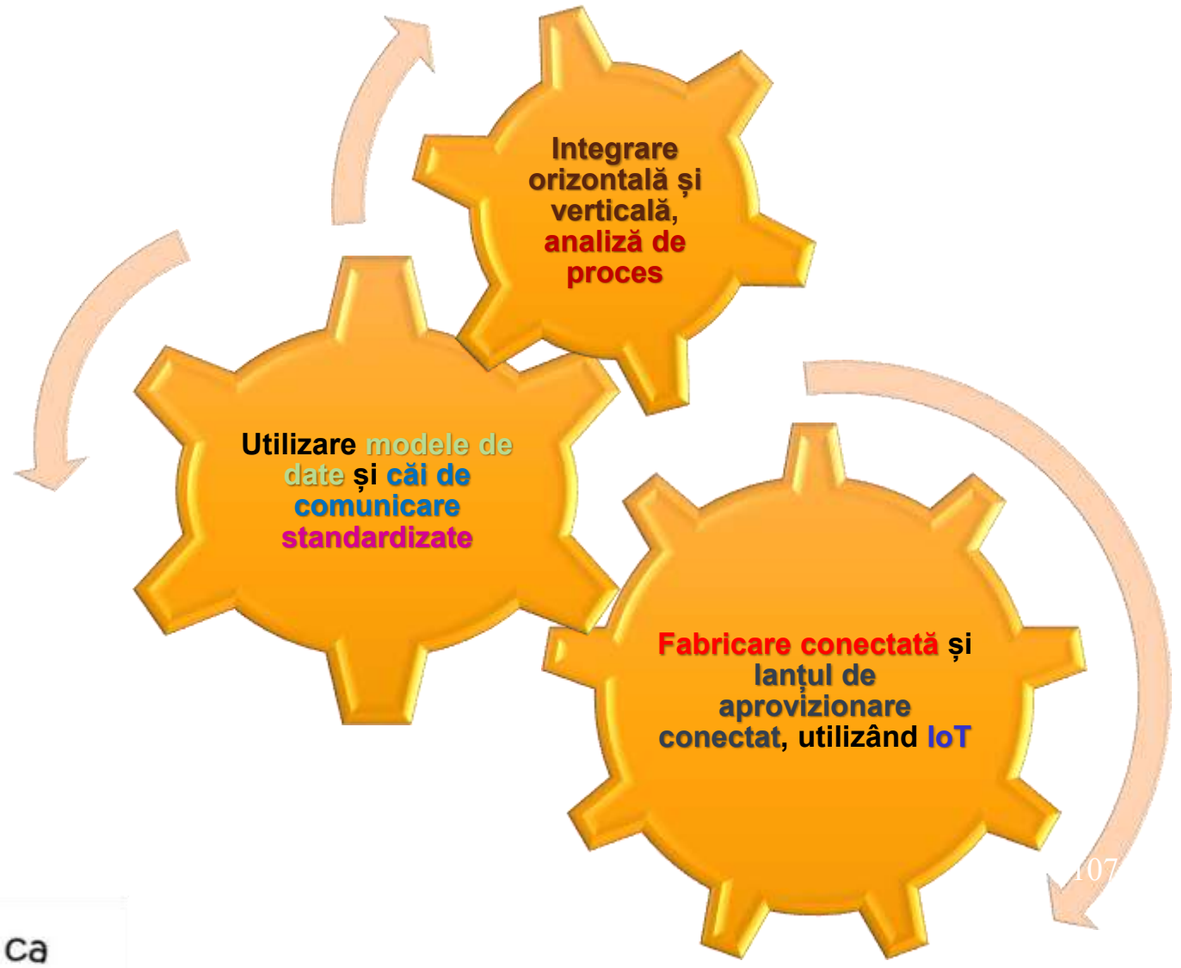
# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ

**2021-prezent**

**Industria 4.0** schimbă complet:
- procesele de producție
- produsele
- relațiile din lanțul de aprovizionare
- modelele de afaceri din companii.

- **Introducerea noilor tehnologii**
- **Interconectare - oameni, mașini și obiecte**

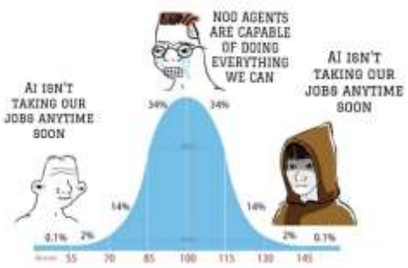
| Companie tradițională | Companie Industrie 4.0 |
|---|---|
| Departamente **separate** | **Departamente interconectate** |
| Dezvoltare produselor și procesele de fabricație sunt **separate** | **Feedback** de la clienți/utilizatori, **colaborare** în rețea |
| **Confuzie și pierdere de informații** | **Sisteme IT integrate** |





**Nu avem nevoie de mai multe instrumente – avem nevoie de o execuție mai bună**


# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ DIN PERSPECTIVĂ ECONOMICĂ




## Plan eficient de investiții în SOLUȚII de securitate cibernetică

**Modul în care un sistem poate funcționa, pe cât de optim este posibil, pe timpul unei perturbări și cum își poate reveni rapid când perturbarea apare**

**Monitorizarea și evaluarea soluțiilor de securitate cibernetică:**
- monitorizare, în mod regulat, eficacitate soluții de securitate cibernetică
- efectuare evaluări periodice ale riscurilor pentru a modificarea/actualizarea soluțiilor de securitate cibernetică și îndeplinirea obiectivelor stabilite

**Planificarea implementării soluțiilor de securitate cibernetică:**
- timp, resurse și personal (propriu / rezervă) necesar
- procese, roluri și responsabilități

**Stabilirea unui buget pentru investiții:**
- calcul costuri curente și recurente măsurilor instituite
- estimare costuri suplimentare pentru implementarea și gestionarea soluțiilor de securitate cibernetică și pentru cazuri neprevăzute

**Identificarea soluțiilor de securitate cibernetică:**
- Identificare soluții conforme cu reglementările
- evaluare comparativă a diferitelor soluții de securitate cibernetică disponibile pe piață (cost, capabilități, scalabilități, flexibilități, etc.)

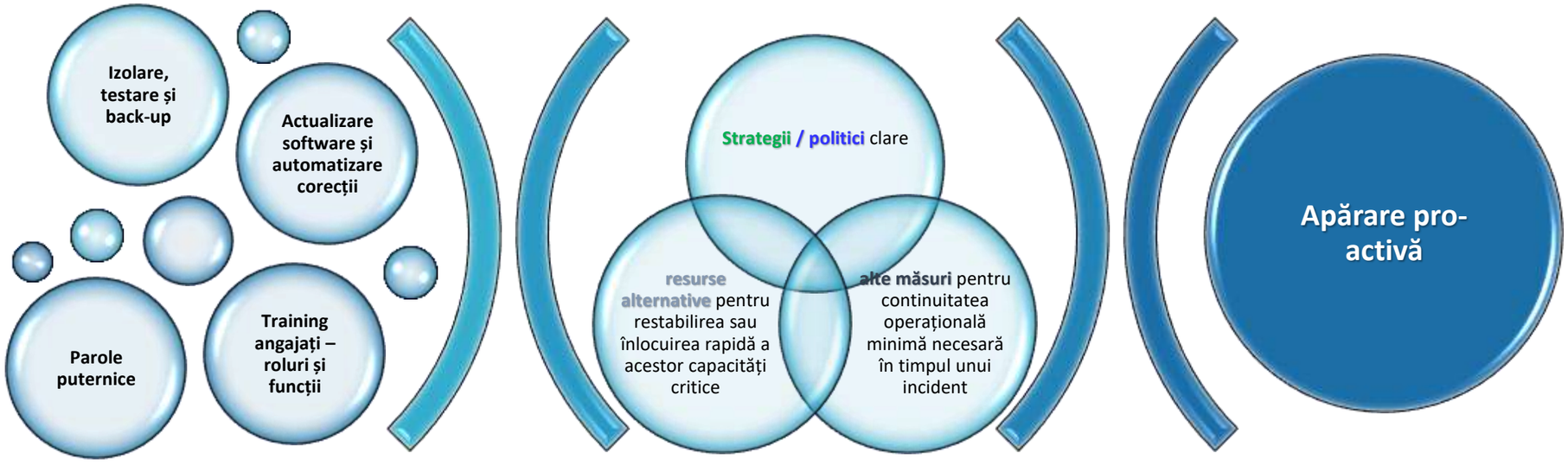
**Definirea obiectivelor de securitate cibernetică:**
- stabilire obiective de securitate cibernetică (clare și specifice)
- ce anume trebuie să fie protejat și de ce


**Evaluarea nevoilor de securitate cibernetică:**
- evaluare riscuri de securitate cibernetică
- identificare zone critice care necesită protecție împotriva amenințărilor cibernetice

**Risc cibernetic** → **Risc de cloud** → **Risc de concentrare (externalizare)** → **Risc de țară**

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ
# DIN PERSPECTIVĂ ECONOMICĂ

## Atitudine proactivă




***Stratificarea protecției în funcție de:***

- ***vectorii de atac***
- ***dispunere geografică / locații***
- ***tip infrastructură (critică)***
- ***categorii (baze) de date***

### Strategii / Politici (clare / îmbunătățite)

**Izolare, testare și back-up**:

- **backup-uri regulate** ale datelor și configurațiilor critice **în medii izolate**
- **segmentare** adecvată **a rețelei / bazelor de date**
- **teste anuale** în condiții reale, verificând capacitatea de restaurare rapidă și completă a sistemelor

Deși **tehnologia cloud facilitează procesele de testare și restaurare**, multe organizații aleg să se concentreze **doar** pe **funcțiile critice**, iar **dezvoltarea unui plan robust de restaurare** – posibil **pe o infrastructură complet separată** – reprezintă o provocare semnificativă care necesită resurse și efort substanțial, în special pentru organizațiile de mari dimensiuni

### Planul de răspuns la incidente / PCA / RDP

**Actualizare software și automatizare corecții**:

- Implementarea unui sistem robust de **management al patch-urilor**
- **proces standardizat** de evaluare regulată a sistemelor pentru identificarea software-ului depășit, testarea patch-urilor în medii controlate și **implementare automată a actualizărilor critice** în afara orelor de program
- **inventar actualizat** active hardware/software/ firmware și **prioritizare patch-uri** în funcție de severitatea vulnerabilităților și criticitatea sistemelor


### confidențialitate, integritate și disponibilitate

Organizația afectată își pierde, adesea, **accesul la**:

- **instrumentele esențiale necesare** pentru investigarea și combaterea atacului însuși
- **sistemele SOC** (Security Operations Center)
- **infrastructura vitală de comunicații și email**, care pot fi compromise sau indisponibile

**set echilibrat de măsuri**

**obligații de reglementare** și **răspuns proactiv la incidente**

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ
# DIN PERSPECTIVĂ ECONOMICĂ


## Atitudine proactivă

**instrument comun** de analiză a riscurilor

dezvoltată de armata SUA din **anii '40**
utilizată de industria aeronautică în **anii '60** (misiunile Apollo) și din **1974** de US Navy și de industria constructoare de mașini

\+

**Instrumente complementare** de analiză a riscurilor

**DIAGRAMĂ DE FLUX**

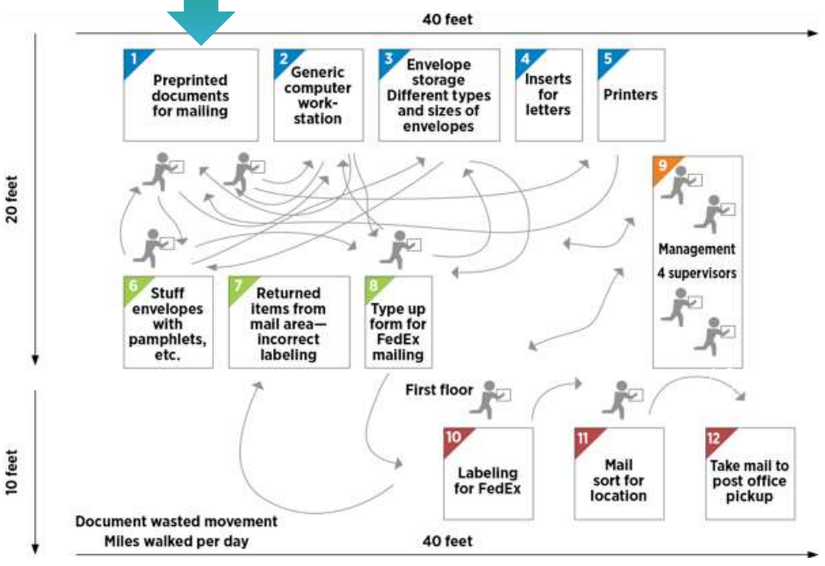
- documentare, înțelege, comunicare mod realizare **proces**
- mai bună comunicare între persoanele implicate în același proces
- studiere proces de îmbunătățire
- planificare **proiect**

**VERIFICAREA ERORILOR (*poka-yoke)*** - dispozitiv sau metode automată de **a face imposibilă apariția unei erori sau ca eroarea să fie imediat evidentă, odată ce a apărut**

- rol de avertizare și/sau control pe parcursul, la transferul ori evaluarea consecințelor unui **proces sau proiect**

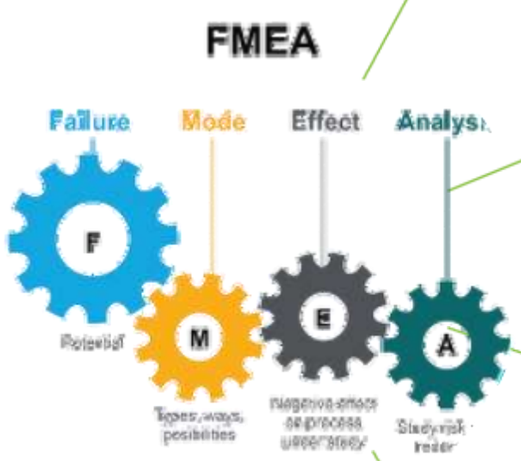
**SPAGHETTI DIAGRAM (diagramă *"de spaghete"*)** - reprezentare vizuală folosind o linie de curgere continuă care **urmărește calea unui articol sau a unei activități printr-un proces**

- identificare **redundanțe** în fluxul de lucru și **oportunități de accelerare** a fluxului de **proces**




**UNDE? CUM? CARE?**

- **abordare sistematică**, pas cu pas
- **identificare și prioritizare posibile defecțiuni** într-un proces, produs sau serviciu de proiectare, fabricație sau asamblare




**Analiza Modurilor de Defectare și a Efectelor (AMDE)**

**Indice de Prioritate al Riscului (IPR) / Număr de Prioritate a Riscului (RPN)**

atenuare / eliminare potențiale eșecuri **(IPR / RPN)**

- **Severitate** efecte asupra consumatorului
- **Probabilitate** apariție
- **Detectabilitate** – cât de ușor poate fi detectată
- **IPR = Severitate x Probabilitate x Detectabilitate**

**îmbunătățește strategiile de gestionare a riscurilor**

**robustețe / fiabilitate** produse și operațiuni

- **„Modul de eșec"** = modul sau maniera în care ceva ar putea eșua
- **"Eșecurile"** = orice erori sau defecte, în special cele care afectează clientul și pot fi potențiale sau reale
- **„Analiza efectelor"** se referă la studierea consecințelor eșecurilor înregistrate

# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ DIN PERSPECTIVĂ ECONOMICĂ

## Modelul Gordon-Loeb

**Cât de mult ar trebui investit în activitățile legate de securitatea cibernetică?**

➡ evaluarea costurilor și beneficiilor (**analiza cost-beneficiu**) **asociate investiției în securitatea cibernetică**


**Prevenire / Constatare**

**Modelul Gordon-Loeb (GL)** - **obținerea nivelului optim (sau cel puțin adecvat) de investiție în securitate cibernetică, în raport cu tipul informațiilor / bazelor de date gestionate (publice / nepublice / clasificate)**

- presupune că, dacă există un anumit **nivel de vulnerabilitate** pentru un **tip de informații**, **investițiile suplimentare în securitate cibernetică** pot aduce **probabilitatea unei încălcări a securității cibernetice să tindă spre zero**, dar **nu zero**

$$z^*(v) < (1/e)vL$$

***e – numărul lui Euler***
*e*≈2,71828 18284 59045 23536

**Factorul uman**

- **nivelul optim de investiție nu ar depăși vL/e**, adică **aproximativ 37% din pierderea așteptată dintr-o încălcare a securității**

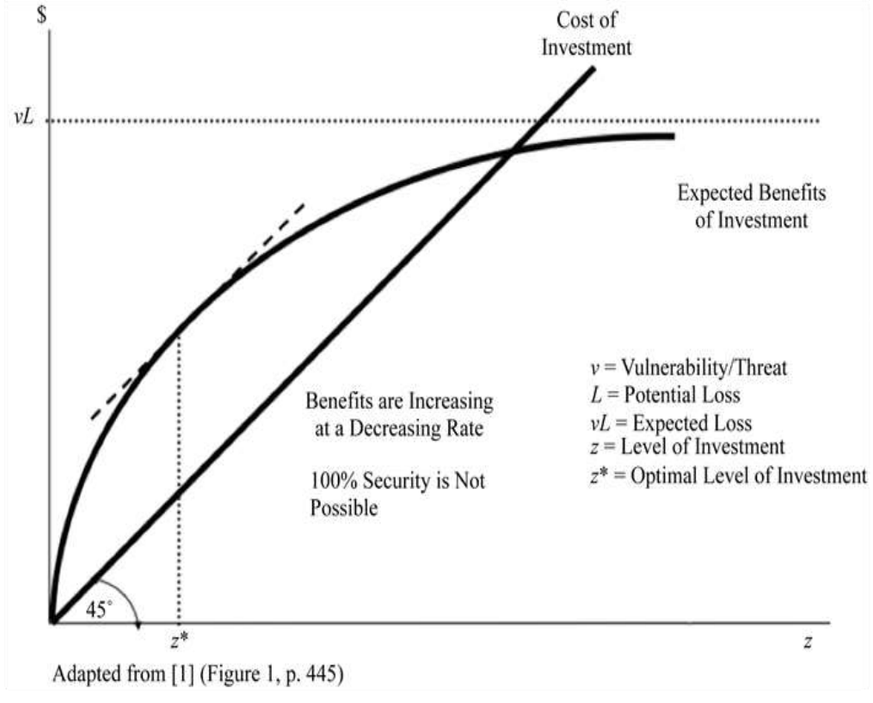
**Willemson și Hausken (2006)** au extins modelul GL pentru **a include diverși factori exogeni**, care nu au fost luați în considerare în modelul original și au demonstrat că **regula 37% nu este întotdeauna valabilă**

- **Furtul de identitate**
- **Furtul de proprietate intelectuală**
- **Atacuri cibernetice asupra infrastructurilor critice**

**Ghid pentru investiții în securitate cibernetică: extensii ale modelului Gordon și Loeb**

*Sursa: https://www.researchgate.net/publication/298736229_Cybersecurity_Investment_Guidance_Extensions_of_the_Gordon_and_Loeb_Model*

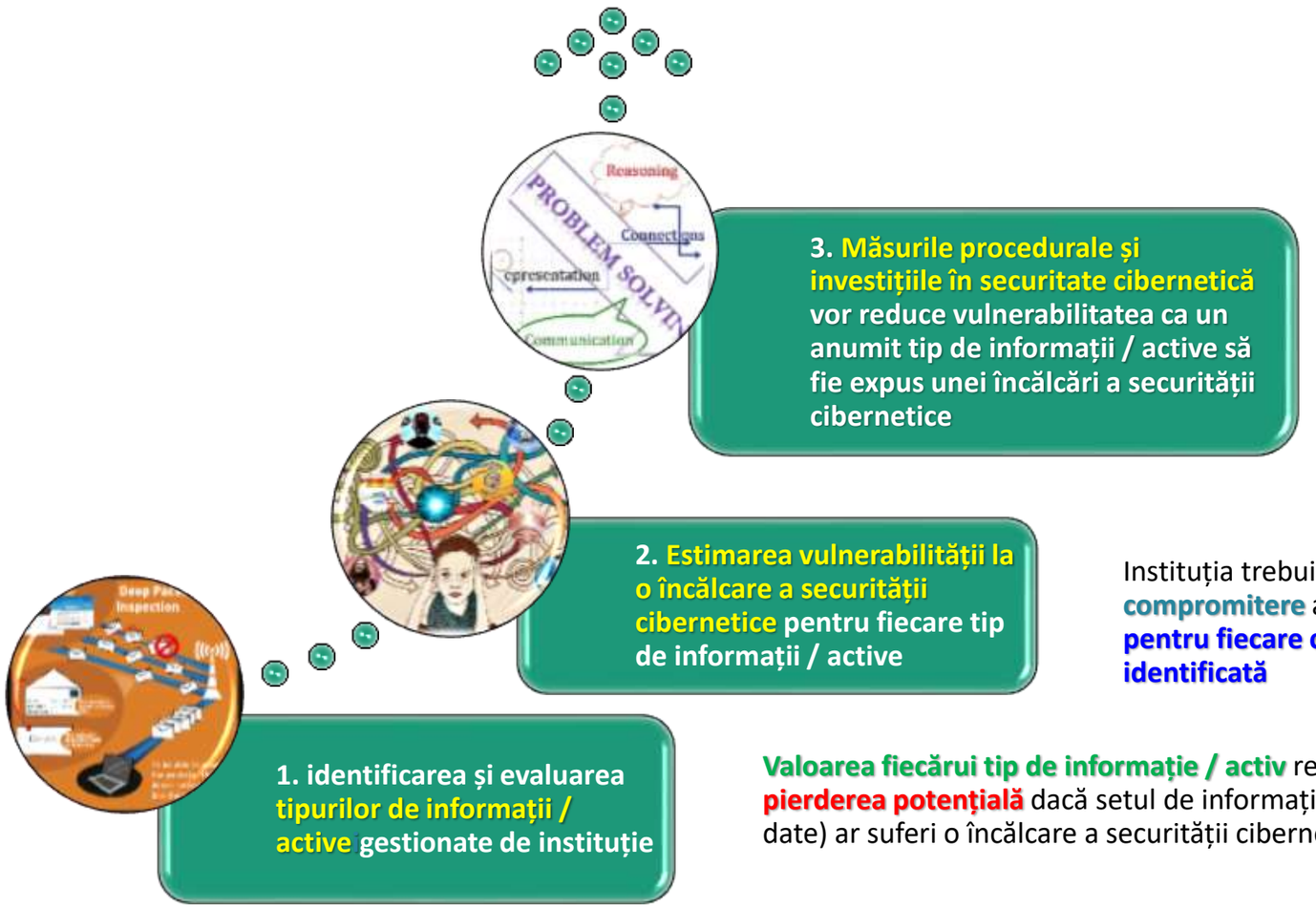
$$z^{SC}(v) < (1/e)\left[1+\left(L^E/L^P\right)\right]vL^P$$




Adapted from [1] (Figure 1, p. 445)


# INVESTIȚIA ÎN SECURITATE CIBERNETICĂ DIN PERSPECTIVĂ ECONOMICĂ

**Rentabilitatea investiției (ROI)** = măsură de performanță utilizată pentru a evalua eficiența sau profitabilitatea unei investiții **(%)**




Instituțiile trebuie să investească, în general, **o sumă care este mai mică sau cel mult egală cu aproximativ 37% din pierderea așteptată** care ar putea rezulta dintr-o încălcare a securității cibernetice a unui tip de informații / active, fiind direct legată de ipoteza că **beneficiile investițiilor în securitate cibernetică cresc într-un ritm descrescător vulnerabillităților**

Instituția trebuie să estimeze **probabilitatea de compromitere** a fiecărui tip de informații / active, **pentru fiecare categorie de informații / active identificată**

**Valoarea fiecărui tip de informație / activ** reprezintă **pierderea potențială** dacă setul de informații (baza de date) ar suferi o încălcare a securității cibernetice

$$\textbf{ROI} = \frac{Valoarea\ curentă\ a\ investiției - Costul\ investiției}{Costul\ investiției} \text{ x } 100\%$$

sau

$$\textbf{ROI} = \frac{FVI - IVI}{Costul\ investiției} \text{ x } 100\%$$

*unde*
*FVI – Valoarea finală a investiției*
*IVI – Valoarea inițială a investiției*


TOSHIBA


„Nu lăsa învățăturile
să devină simple
cunoștințe.
Transformă-le
în acțiuni.”
John C. Maxwell
JOHN MAXWELL Team.RO