ANALIZĂ CONTRASTIVĂ DE CONVERGENȚĂ A RISCURILOR, DE EFICIENȚĂ OPERAȚIONALĂ ȘI DE CONFORMITATE STANDARDIZATĂ· SECURITATE FIZICĂ ȘI GUVERNANȚĂ TEHNOLOGICĂ

DE LA PANOPTIC LA AGENT AUTONOM: RECONFIGURAREA GLOBALĂ A SECURITĂȚII FIZICE ÎN ERA INTELIGENȚEI ARTIFICIALE ȘI RESTANȚELE STRUCTURALE ALE CADRULUI ROMÂNESC

SERIE ÎN PATRU PĂRȚI · PARTEA I DIN IV
STUDIU COMPARATIV · SECURITATE FIZICĂ ȘI GUVERNANȚĂ TEHNOLOGICĂ
Publicație de specialitate · Domeniul evaluării de risc la securitate fizică

EXPLOZIA TEHNOLOGICĂ A SECURITĂȚII FIZICE: CHINA, STATELE UNITE ȘI UNIUNEA EUROPEANĂ ÎN ERA INTELIGENȚEI ARTIFICIALE

LĂZĂU ANGELO *— evaluator de risc la securitate fizică, la* ***WORLD CLASS LA-INT&SECRSK CONSULTANCY****, înscris în Registrul Național al Evaluatorilor de Risc la Securitate Fizică* ***(R.N.E.R.S.F.)****; cu experiență anterioară în structuri militare de informații și securitate, precum și în funcția de* ***Head of Security*** *al unei entități* ***NATO*** *din România — o combinație între practica de teren, cultura de securitate a alianței și cadrul juridic autohton al profesiei.*

Argument

Acesta este primul dintr-o serie de patru articole care examinează, împreună, transformarea securității fizice sub presiunea convergenței dintre supravegherea video, controlul accesului și inteligența artificială. Acest episod urmărește trei arhitecturi de guvernanță — China, Statele Unite și Uniunea Europeană — susținute de literatura corporativă și de reglementare din 2025–2026, și introduce o categorie de risc emergentă: identitățile non-umane. Episoadele următoare aduc discuția în plan național, examinând cadrul legal românesc, incidentele care îi documentează limitele, mecanismele concrete de atac și implicațiile juridice pentru profesia de evaluator de risc.

Cuvinte-cheie: securitate fizică, inteligență artificială, identități non-umane, AI Act, guvernanță tehnologică, China, Statele Unite, Uniunea Europeană.

Explozia tehnologică a securității fizice în era cibernetică și a inteligenței artificiale

Pentru cea mai mare parte a istoriei sale moderne, securitatea fizică a fost o disciplină a materiei: garduri, încuietori, grilaje, senzori de mișcare, cabluri de cupru. Ultimii cinci ani au produs o ruptură de paradigmă pe care literatura de specialitate a marilor producători o descrie, fără rezerve retorice, drept trecerea de la „sisteme care înregistrează” la „sisteme care decid”. Rapoartele anuale ale companiilor Axis Communications, Genetec, Hanwha Vision și Motorola Solutions, publicate la finalul lui 2025 și pe parcursul lui 2026, converg spre același diagnostic: inteligența artificială a încetat să fie un modul opțional atașat unei camere video și a devenit arhitectura însăși a sistemului de securitate.[1]

[1]Axis Communications, „Five Key Technology Trends Affecting the Security Sector in 2026”, Euro Security, 2 decembrie 2025; Genetec Inc., 2026 Global State of Physical Security Report, decembrie 2025; sinteză publicată de asmag.com, „Top Brands Share Their Views on Physical Security Trends in 2026”, 2026.

Pentru cea mai mare parte a istoriei sale moderne, securitatea fizică a fost o disciplină a materiei: garduri, încuietori, grilaje, senzori de mișcare, cabluri de cupru. Ultimii cinci ani au produs o ruptură de paradigmă pe care literatura de specialitate a marilor producători o descrie, fără rezerve retorice, drept trecerea de la „sisteme care înregistrează” la „sisteme care decid”. Rapoartele anuale ale companiilor Axis Communications, Genetec, Hanwha Vision și Motorola Solutions, publicate la finalul lui 2025 și pe parcursul lui 2026, converg spre același diagnostic: inteligența artificială a încetat să fie un modul opțional atașat unei camere video și a devenit arhitectura însăși a sistemului de securitate.[2]

China: standardizare de stat și supraveghere la scară urbană

China rămâne, prin volum de piață și densitate de instalare, cel mai mare laborator global al securității fizice bazate pe AI. Hikvision și Dahua Technology, companii care, împreună cu Uniview, controlează aproape 59% din piața internă chineză de supraveghere video, au trecut, în ultimii doi ani, de la simpla înregistrare video la platforme integrate de analiză comportamentală: recunoaștere de obiecte, detecție de anomalii, recunoaștere facială la scară de oraș. Programul „Xueliang” (Ochii Ageri), care ancorează cererea internă de infrastructură video de siguranță publică prin aproape 800 de proiecte-pilot de oraș inteligent, ilustrează un model în care securitatea fizică privată și supravegherea de stat operează pe aceeași infrastructură tehnică.[3]

Această expansiune comercială a fost dublată, în 2026, de un efort de standardizare fără precedent. Comitetul Național pentru Standardizarea Securității Cibernetice (TC260) a publicat, în iulie 2026, un proiect de standard privind clasificarea și gradarea riscului aplicațiilor de inteligență artificială, care extinde explicit analiza de risc dincolo de securitatea datelor, incluzând siguranța fizică și influența cognitivă drept categorii distincte de risc de evaluat. Este o recunoaștere oficială a exact fenomenului pe care acest articol îl tratează: sistemele de securitate fizică bazate pe AI nu mai pot fi evaluate izolat de infrastructura lor digitală.[4]

Notă de context. Piața internă chineză de AI a depășit un trilion de yuani (139,2 mld. $ / 123,1 mld. €) în 2025, cu peste 5.300 de companii active pe lanțul de la infrastructură la aplicație, o scară care explică ritmul accelerat al standardizării TC260 și presiunea de a reglementa retroactiv o industrie deja matură.[5]

[2]Axis Communications, „Five Key Technology Trends Affecting the Security Sector in 2026”, Euro Security, 2 decembrie 2025; Genetec Inc., 2026 Global State of Physical Security Report, decembrie 2025; sinteză publicată de asmag.com, „Top Brands Share Their Views on Physical Security Trends in 2026”, 2026.

[3]Mordor Intelligence, China Video Surveillance Market — Size, Analysis, Outlook & Share Report, ianuarie 2026; date privind cotele de piață ale Hikvision, Dahua Technology și Uniview, și privind Proiectul „Xueliang” (Sharp Eyes).

[4]China Briefing, „China Releases Draft Standard on AI Application Security Classification and Grading”, iulie 2026 — proiect de standard al Comitetului Național pentru Standardizarea Securității Cibernetice (TC260).

[5]China Briefing, op. cit.; date privind piața internă chineză de AI raportate de China Academy of Information and Communications Technology (CAICT), 2025.

Statele Unite: inovație privată, reglementare sectorială și tensiunea geopolitică a lanțului de aprovizionare

Modelul american este, structural, opus celui chinez: inovația precede reglementarea, iar statul intervine sectorial și, adesea, din motive de securitate națională mai degrabă decât de protecție a consumatorului. Motorola Solutions, prin achiziția Avigilon și Honeywell rămân actori dominanți în platformele integrate de securitate corporativă, dar literatura sectorială din 2026 arată o schimbare de fond: pentru prima dată, inteligența artificială a intrat în topul priorităților de proiect alături de controlul accesului și supravegherea video, iar interesul utilizatorilor finali pentru adoptarea AI s-a dublat față de anul anterior. Aproximativ 70% dintre respondenți își exprimă însă rezerve explicite privind modul în care sunt proiectate și implementate sistemele AI, un decalaj de încredere pe care doar o cincime dintre organizații îl declară absent.[6,7]

Dimensiunea geopolitică nu poate fi separată de cea tehnologică. Secțiunea 889 din legea federală a autorizațiilor de apărare (NDAA) interzice, din 2019, achiziția de echipamente Hikvision și Dahua de către agențiile federale americane și contractorii acestora, iar noua generație a NDAA, adoptată pentru 2026, extinde mandatul Centrului de Securitate AI din cadrul Agenției Naționale de Securitate pentru protejarea tehnologiilor AI avansate împotriva furtului sau sabotajului de către actori statali. Practic, alegerea unui furnizor de camere video sau de control acces a devenit, pentru operatorii de infrastructură critică americană, o decizie de securitate națională, nu doar una tehnică.[8]

Uniunea Europeană: guvernanță dinspre drepturile fundamentale

Europa a ales un punct de plecare normativ, nu comercial. Regulamentul privind inteligența artificială (AI Act), ale cărui obligații pentru sistemele cu risc ridicat au fost reașezate prin Regulamentul (UE) 2026/1744, în vigoare din 27 iulie 2026 — 2 decembrie 2027 pentru sistemele autonome din Anexa III și 2 august 2028 pentru cele integrate în produse reglementate (Anexa I), în timp ce obligațiile de transparență din art. 50 se aplică, în principal, din 2 august 2026 —, clasifică drept „risc ridicat” exact categoriile de sisteme pe care industria securității fizice le vinde cel mai activ: identificarea biometrică, categorisirea persoanelor, recunoașterea emoțiilor, managementul infrastructurii critice. Obligațiile care urmează să se aplice nu sunt declarative: evaluare de conformitate, înregistrare în baza de date UE, marcaj CE, guvernanța datelor de antrenament, supraveghere umană documentată și, potrivit Articolului 15, rezistență demonstrabilă la atacuri adversariale asupra întregului lanț de acțiune al sistemului, nu doar asupra rezultatului algoritmului.[9]

---

[6] Genetec Inc., 2026 Global State of Physical Security Report; preluat în Campus Safety Magazine, „Genetec Releases 2026 Global State of Physical Security Report Findings”, 18 decembrie 2025.

[7] Genetec Inc., webinar „Trends Shaping Physical Security in 2026”, 2026; Security Sales & Integration, „Genetec Releases 2026 Global State of Physical Security Report”, 9 decembrie 2025.

[8] Lawfare Media, „Latest NDAA Supports AI Safety, Innovation, and China Decoupling”, 5 februarie 2026.

[9] Responsible AI Labs (RAIL), „EU AI Act August 2026: Your Compliance Countdown”, 2026; Salt Security, „EU AI Act Compliance 2026: What High-Risk AI Systems Must Do Now”, 28 mai 2026.

Producători precum Axis Communications au integrat această presiune normativă direct în discursul tehnologic: raportul privind tendințele tehnologice pentru 2026 al companiei suedeze plasează arhitectura „zero-trust", în care fiecare dispozitiv, utilizator și conexiune trebuie autentificat continuu, drept standard implicit pentru orice sistem de securitate fizică nou proiectat, alături de actualizări automate de firmware și gestionarea criptografică a identității fiecărui echipament. Este semnificativ că, la finalul lunii aprilie 2026, o proporție majoritară a organizațiilor europene nu finalizase pregătirile de conformitate, un decalaj de implementare pe care industria îl numește, fără eufemisme, „cea mai îngustă fereastră de planificare din istoria recentă a sectorului".[10,11]

Identitățile non-umane: frontiera invizibilă a riscului

Convergența dintre cele trei modele generează o categorie de risc pe care metodologiile clasice de analiză nu o anticipează: identitățile non-umane (non-human identities). Fiecare cameră video conectată la cloud, fiecare modul de analiză comportamentală, fiecare agent AI care gestionează automat drepturile de acces reprezintă, tehnic, un „utilizator" care acționează fără parolă introdusă manual și fără sesiune închisă la finalul programului. Rapoarte sectoriale din prima jumătate a lui 2026 documentează un raport de până la 80 de identități non-umane la un singur angajat uman, într-o organizație medie, o cifră care, translatată în limbajul evaluării de risc la securitate fizică, înseamnă că perimetrul digital al unui obiectiv păzit este, statistic, de zeci de ori mai extins decât perimetrul fizic pe care evaluatorul îl inspectează.[12]

Implicație directă. Un agent AI compromis nu așteaptă o fereastră de oportunitate ca un intrus uman: acționează la viteza rețelei. O cheie de acces API expusă într-un depozit de cod configurat greșit poate produce, tehnic, exact același rezultat ca o efracție reușită, deschiderea unei uși, dezactivarea unei alarme, ștergerea unei înregistrări, fără ca vreun gard sau lacăt să fi cedat.

Bibliografie

Lucrarea urmează convenția citării prin note de subsol numerotate. Referințele de mai jos acoperă exclusiv sursele folosite în acest episod; bibliografia completă a seriei apare, cumulativ, la finalul Părții a IV-a.

B. Rapoarte instituționale și corporative

Axis Communications, Five Key Technology Trends Affecting the Security Sector in 2026, Euro Security, 2 decembrie 2025.

[10] Axis Communications, op. cit., Euro Security, 2 decembrie 2025.

[11] Responsible AI Labs (RAIL), op. cit. — potrivit sursei citate, 78% dintre organizațiile europene nu finalizaseră, la aprilie 2026, pași semnificativi de conformare cu AI Act.

[12] KPMG International, Cybersecurity Considerations 2026; preluat în nhimg.org, „KPMG 2026 Cybersecurity Report Identifies Non-Human Identities as a Critical Priority for CISOs", 5 iunie 2026; Cloud Security Alliance & Oasis Security, raport comun privind identitățile non-umane (NHI) și securitatea AI, 2026.

China Briefing, China Releases Draft Standard on AI Application Security Classification and Grading, iulie 2026.

Cloud Security Alliance & Oasis Security, State of NHI and AI Security Report, 2026.

Genetec Inc., 2026 Global State of Physical Security Report, decembrie 2025.

KPMG International, Cybersecurity Considerations 2026, 2026.

Mordor Intelligence, China Video Surveillance Market — Size, Analysis, Outlook & Share Report, ianuarie 2026.

Responsible AI Labs (RAIL), EU AI Act August 2026: Your Compliance Countdown, 2026.

Salt Security, EU AI Act Compliance 2026: What High-Risk AI Systems Must Do Now, 28 mai 2026.

Regulamentul (UE) 2026/1744 de modificare a Regulamentului (UE) 2024/1689 (AI Act), în vigoare din 27 iulie 2026; Steptoe, EU AI Act Amendments Enter Into Force, 2026.

C. Articole de presă și analize de specialitate

Campus Safety Magazine, „Genetec Releases 2026 Global State of Physical Security Report Findings”, 18 decembrie 2025.

Lawfare Media, „Latest NDAA Supports AI Safety, Innovation, and China Decoupling”, 5 februarie 2026.

nhimg.org, „KPMG 2026 Cybersecurity Report Identifies Non-Human Identities as a Critical Priority for CISOs”, 5 iunie 2026.

Security Sales & Integration, „Genetec Releases 2026 Global State of Physical Security Report”, 9 decembrie 2025.

D. Surse electronice principale

asmag.com — „Top Brands Share Their Views on Physical Security Trends in 2026 — Manufacturer Roundtable”, 2026.

ANALIZĂ CONTRASTIVĂ DE CONVERGENȚĂ A RISCURILOR, DE EFICIENȚĂ OPERAȚIONALĂ ȘI DE CONFORMITATE STANDARDIZATĂ· SECURITATE FIZICĂ ȘI GUVERNANȚĂ TEHNOLOGICĂ

DE LA PANOPTIC LA AGENT AUTONOM: RECONFIGURAREA GLOBALĂ A SECURITĂȚII FIZICE ÎN ERA INTELIGENȚEI ARTIFICIALE ȘI RESTANȚELE STRUCTURALE ALE CADRULUI ROMÂNESC

SERIE ÎN PATRU PĂRȚI · PARTEA A II-A DIN IV

Publicație de specialitate · Domeniul evaluării de risc la securitate fizică

ROMÂNIA: O METODOLOGIE SOLIDĂ BLOCATĂ ÎNTR-O ERĂ PRE-DIGITALĂ

***LĂZĂU ANGELO** — evaluator de risc la securitate fizică, la **WORLD CLASS LA-INT&SECRSK CONSULTANCY**, înscris în Registrul Național al Evaluatorilor de Risc la Securitate Fizică **(R.N.E.R.S.F.)**; cu experiență anterioară în structuri militare de informații și securitate, precum și în funcția de **Head of Security** al unei entități **NATO** din România — o combinație între practica de teren, cultura de securitate a alianței și cadrul juridic autohton al profesiei.*

Argument

Al doilea episod al seriei aduce discuția în plan național, examinând decalajul dintre ritmul transformării tehnologice descrise în Partea I și cadrul legal românesc, rămas structural neschimbat din 2003–2012. O secțiune dedicată analizează Ordonanța de urgență nr. 37/2026, prima intervenție legislativă recentă asupra Legii nr. 333/2003, arătând distanța dintre recunoașterea declarativă a presiunii tehnologice, prezentă în expunerea de motive, și conținutul ei normativ efectiv, limitat la aspecte administrativ-organizatorice. Discuția este susținută de cinci incidente fizice concrete din România — patru cazuri clasice și jaful de la Poșta Mare din Timișoara, unde a fost confirmată prima utilizare românească a bruiajului RF pentru neutralizarea unei alarme.

Cuvinte-cheie: securitate fizică, Legea 333/2003, O.U.G. 37/2026, analiză de risc, evaluator de risc, incidente de securitate, bruiaj RF.

Acest al doilea episod al seriei continuă direct de unde s-a oprit Partea I, care a urmărit transformarea globală a securității fizice sub presiunea convergenței dintre supraveghere, control acces și inteligență artificială, în China, Statele Unite și Uniunea Europeană. Episodul de față aduce discuția în plan național.

Contrastul dintre viteza descrisă mai sus și realitatea normativă românească este, la o privire academică lipsită de complezență, brutal. Cadrul legal fundamental al evaluării de risc la securitate fizică din România, Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor și Normele metodologice aprobate prin H.G. nr. 301/2012 au fost gândite într-o epocă în care „sistem electronic de securitate” însemna, în esență, o centrală de alarmă cu fir, un set de detectoare de mișcare și un dispecerat telefonic. Legea are, la acest moment, peste două decenii; normele metodologice de aplicare, peste un deceniu. Niciunul dintre cele două acte normative nu menționează, măcar tangențial, inteligența artificială, identitățile non-umane, integrarea cloud sau riscul

cibernetic asociat unui sistem electronic de securitate, deși acesta din urmă este, în 2026, arhitectura implicită a oricărui sistem nou instalat.[13]

Această restanță normativă nu este doar o chestiune de eleganță legislativă. Ea produce un decalaj practic: evaluatorul de risc este obligat, prin instrucțiunile de aplicare, să raporteze la o anexă de cerințe minime de securitate gândită pentru o generație tehnologică depășită, în timp ce proiectantul și instalatorul lucrează, în teren, cu echipamente ale căror vulnerabilități reale se află în stratul digital pe care legea nu-l reglementează.[14]

Ordonanța de urgență nr. 37/2026: retorica tehnologică și substanța administrativă

Dacă secțiunea precedentă ar putea lăsa impresia unei simple neglijențe legislative, evoluția recentă a cadrului normativ arată ceva mai grav: o conștientizare oficială a problemei, urmată de o intervenție care o ocolește aproape în totalitate. La 4 mai 2026, Guvernul României a adoptat Ordonanța de urgență nr. 37/2026 pentru modificarea și completarea Legii nr. 333/2003, publicată în Monitorul Oficial, Partea I, nr. 381 din 6 mai 2026 și intrată în vigoare la aceeași dată. Actul a fost adoptat, ca orice ordonanță de urgență, în temeiul art. 115 alin. (4) din Constituție, care impune invocarea unei „stări de fapt obiective, cuantificabile, extraordinare”, a cărei reglementare nu poate fi amânată. La nivel declarativ, printre argumentele care susțin acest caracter extraordinar figurează exact temele tratate în secțiunea I a acestui articol: accelerarea tehnologică, apariția inteligenței artificiale și expunerea tot mai mare a infrastructurilor de securitate la riscuri de natură cibernetică. Este, în sine, un moment de validare: pentru prima dată, un act normativ românesc din domeniul pazei și protecției recunoaște explicit, în expunerea de motive, existența acestei presiuni tehnologice.[15]

Distanța dintre această recunoaștere declarativă și conținutul normativ efectiv al ordonanței este însă considerabilă. O lectură articol cu articol a O.U.G. nr. 37/2026 scoate la iveală o listă de modificări exclusiv organizatorice și procedurale: introducerea unor categorii noi de pază cu efective de jandarmi: pază de proximitate, temporară și permanentă, restrângerea obligativității avizului de poliție pentru planul de pază doar la obiectivele cu pază înarmată, înființarea unui regim de înregistrare națională a evaluatorilor de risc la securitate fizică însoțit de o interdicție de a evalua obiective cu care propria firmă are relații contractuale, introducerea unor cazuri exprese în care poliția poate anula o analiză de risc întocmită pe date eronate sau fără inspectarea efectivă a obiectivului, un prag minim de trei agenți de pază, dintre care cel puțin unul înarmat pentru

[13]Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, republicată în Monitorul Oficial al României, Partea I, nr. 189 din 18 martie 2014, cu modificările și completările ulterioare; Hotărârea de Guvern nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003, publicată în Monitorul Oficial, Partea I, nr. 335 din 17 mai 2012.

[14]Instrucțiunile nr. 9 din 1 februarie 2013 ale Inspectoratului General al Poliției Române privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003.

[15]Ordonanța de urgență nr. 37/2026 pentru modificarea și completarea Legii nr. 333/2003, publicată în Monitorul Oficial al României, Partea I, nr. 381 din 6 mai 2026; text disponibil pe Portal Legislativ, legislatie.just.ro, și pe Lege5.ro.

transporturile de valori în interiorul localităților, precum și un set de reguli privind uniformele, siglele înregistrate și interdicția purtării măștii de către personalul de pază, dublate de un nomenclator nou de contravenții.[16]

Ce lipsește din O.U.G. nr. 37/2026. În cele peste 25 de puncte de modificare ale ordonanței nu apare niciun articol care să reglementeze componenta digitală a sistemelor electronice de securitate: nicio mențiune despre conectivitate cloud, despre securitatea cibernetică a centralelor de alarmă conectate la rețea, despre criteriile de evaluare a riscului asociat inteligenței artificiale integrate în camerele video sau despre identitățile non-umane care operează, în prezent, o parte semnificativă a echipamentelor instalate. Singura legătură cu digitalul este de natură administrativă , registrul național al evaluatorilor, nu tehnică.

Semnificativ este și articolul din dispozițiile finale ale ordonanței (art. VI), care obligă Guvernul ca, în termen de 90 de zile de la intrarea în vigoare, respectiv până la 4 august 2026, să modifice în mod corespunzător Normele metodologice de aplicare a Legii nr. 333/2003, aprobate prin H.G. nr. 301/2012. Formularea „în mod corespunzător” este relevantă: viitoarea modificare a normelor metodologice este gândită, prin chiar textul ordonanței, ca o simplă armonizare structurală cu noile categorii introduse în lege, tipurile de pază, regimul avizării, registrul evaluatorilor, nu ca o oportunitate de a introduce, în anexele tehnice, o metodologie de evaluare a riscului digital. Termenul a fost depășit: potrivit presei de specialitate, la 11 septembrie 2026 proiectul de modificare nu fusese publicat, iar normele nu erau adoptate; întârzierea nu suspendă ordonanța, termenul fiind unul adresat Guvernului. Contrastul cu agenda europeană rămâne grăitor: la nivelul Uniunii, calendarul AI Act a fost reașezat prin Regulamentul (UE) 2026/1744 (2 decembrie 2027 pentru Anexa III, 2 august 2028 pentru Anexa I), în timp ce România nu și-a actualizat încă nici normele de aplicare ale unei legi din 2003. Cu alte cuvinte, viitoarea H.G. de modificare a normelor va reproduce, cel mai probabil, exact aceeași logică declarativ-tehnologică, dar substanțial-administrativă, care caracterizează deja O.U.G. nr. 37/2026.[17]

Consecința practică a acestei alegeri legislative — o ordonanță de urgență succesivă, cu modificări punctuale ale unei legi din 2003, în locul unei legi noi cu norme de aplicare gândite de la zero pentru era digitală se transferă direct asupra celor patru actori ai lanțului profesional. Evaluatorul de risc rămâne obligat să raporteze la o anexă de cerințe minime care nu recunoaște riscul digital ca variabilă de evaluare; proiectantul nu are, în continuare, niciun reper normativ care să-i impună documentarea arhitecturii de rețea sau a dependențelor cloud ale sistemului proiectat; instalatorul nu este ținut, prin nicio normă tehnică obligatorie, să securizeze componentele conectate ale sistemului; iar beneficiarul final rămâne expus unui risc pe care legea încă nu-l denumește, dar pe care îl va suporta

[16] O.U.G. nr. 37/2026, op. cit.; analiză a conținutului normativ în Revista Universul Juridic, „Legea nr. 333/2003 ... modificări (O.U.G. nr. 37/2026)”, 12 mai 2026, și arts.org.ro, „Modificarea Legii nr. 333/2003 prin OUG 37 din 4 mai 2026”, 12 mai 2026.

[17] O.U.G. nr. 37/2026, dispoziții finale privind termenul de 90 de zile pentru modificarea Normelor metodologice aprobate prin H.G. nr. 301/2012, text conform Portal Legislativ, legislatie.just.ro.

integral în bani, în bunuri, în valori în momentul în care un incident de securitate își are originea nu în gard sau în lacăt, ci în stratul digital al propriului sistem de protecție. Sarcina financiară și materială a acestei restanțe legislative nu cade, așadar, asupra statului care a amânat reglementarea, ci asupra beneficiarului care a plătit pentru un sistem modern, crezând, în mod rezonabil, că acesta este evaluat, proiectat și reglementat la fel de modern.

Alegerea repetată a ordonanței de urgență instrument prin definiție punctual și reactiv în locul unei legi noi, însoțite de norme de aplicare integral rescrise, spune, ea însăși, ceva despre modul în care este gestionată, la nivel de politică publică, această tranziție tehnologică. O lege nouă ar fi permis o regândire de fond a anexelor tehnice, a categoriilor de risc și a competențelor profesionale cerute evaluatorilor, proiectanților și instalatorilor, în acord cu exact transformarea descrisă în secțiunea I a acestui articol. O succesiune de ordonanțe care „modifică și completează” un schelet normativ din 2003 nu poate produce acest rezultat, indiferent de câte ori este repetată poate doar amâna, cu fiecare intervenție, momentul în care decalajul devine, pentru un beneficiar concret, un incident real.

Incidente care documentează decalajul

Decalajul nu este teoretic. Cazuistica ultimilor ani din România oferă exemple concrete în care fisura nu a fost în perimetrul fizic, ci în operarea sau proiectarea sistemului de securitate exact zona pe care o analiză de risc actualizată ar fi trebuit să o acopere.

Cazul 1 — Iași, septembrie 2024. Într-o sucursală bancară, un atacator mascat, având asupra sa un obiect asemănător unei arme, a amenințat angajații și a cerut bani. Potrivit informațiilor publice, alerta la 112 a fost transmisă abia la 40 de minute după incident, iar butonul de panică nu a fost acționat, reprezentanții băncii invocând motive de natură juridică. Cazul ilustrează un eșec de procedură operațională a beneficiarului nu de echipament, exact tipul de vulnerabilitate pe care o analiză de risc trebuie să o identifice și pe care o instruire adecvată a personalului trebuie să o elimine.[18]

Cazul 2 — Călărași, decembrie 2024. Un jaf armat asupra unei sucursale bancare a durat, potrivit imaginilor de supraveghere făcute publice, aproximativ 40 de secunde interval în care autorul a amenințat angajații și a părăsit incinta cu o sumă importantă de bani, fără a fi identificat la momentul relatărilor publice. Durata extrem de scurtă a incidentului pune sub semnul întrebării eficiența reală a măsurilor de temporizare și a procedurilor de reacție prevăzute în analiza de risc a obiectivului.[19]

Cazul 3 — Cluj-Napoca, jaful de la Banca Transilvania. Într-un incident de referință în istoria securității bancare românești, autoritățile de la acel moment au criticat public

[18]Digi24, „Jaf armat într-o bancă din Iași, făptașul e de negăsit”, 27 septembrie 2024; Realitatea.net, „Panică la o sucursală bancară din Iași”, 26 septembrie 2024.
[19]Observator News, „Jaful de la banca din Călărași, filmat”, 4 decembrie 2024; Click.ro, „Jaf armat la o bancă din România”, 4 decembrie 2024.

absența unui sistem dublu de uși („mantrap") la unitatea vizată, calificând situația drept inadmisibilă pentru un sediu bancar. Banca a susținut, la rândul ei, că nivelul de securitate implementat era standard pentru sector un argument care, el însuși, expune o problemă structurală: „standardul de sector" poate fi, sistemic, insuficient dacă analiza de risc individuală a fiecărui obiectiv nu îl corectează.[20]

Cazul 4 — Sibiu, noiembrie 2023. Un antreprenor a fost atacat în propria locuință de trei persoane mascate, care au recurs la violență fizică și au amenințat cu o armă membrii familiei acestuia. Cazul, produs la doar câteva zile înaintea unui alt incident grav petrecut aceluiași om de afaceri, arată limitele unei analize de risc rezidențiale care nu a anticipat un profil de amenințare personalizat, adaptat statutului și expunerii publice a beneficiarului.[21]

Cazul 5 — Poșta Mare Timișoara, mai 2025. Trei persoane au pătruns prin efracție în sediul central al Poștei Române din Timișoara și au sustras aproape 9,47 milioane de lei, destinați plății pensiilor. Pentru a neutraliza sistemul de alarmă, infractorii au folosit un dispozitiv de bruiaj RF cu 16 antene, de proveniență chineză, cumpărat online — deși importul, deținerea și utilizarea unor asemenea dispozitive sunt interzise în România prin H.G. nr. 740/2016. Bruiajul a funcționat tehnic impecabil: alarma nu s-a declanșat. Autorii au fost prinși, totuși, la scurt timp — nu printr-o breșă a planului lor tehnic, ci printr-un control de rutină al Poliției Rutiere, complet independent de sistemul electronic de securitate al obiectivului; o anchetă ulterioară a stabilit și complicitatea unei angajate a Poștei. Este primul caz public din România în care metoda de operare descrisă în secțiunea III.1 pentru piețele americană și britanică — bruiajul RF ca instrument de neutralizare a alarmelor — este confirmată, cu succes tehnic, pe teritoriul național.[22]

Cazurile 1–4 nu au fost cauzate, în mod direct, de o tehnologie AI sau de o breșă tehnică sofisticată — sunt eșecuri de procedură, de instruire și de o metodologie de evaluare care nu a privit încă dincolo de gard. Cazul 5 schimbă însă radical premisa: arată că exact tehnica de vârf documentată în secțiunea următoare pentru piețele occidentale bruiajul RF, ca instrument de neutralizare a alarmelor — nu mai este un scenariu de import ipotetic pentru România, ci un eveniment deja produs, anchetat și sancționat definitiv de o instanță. Tocmai de aceea, decalajul normativ descris în această secțiune este cu atât mai periculos: sistemele electronice instalate în ultimii ani integrează, tot mai frecvent, componente cloud și analiză video inteligentă, fără ca metodologia de evaluare a riscului, formarea profesională a evaluatorilor sau procedurile de operare ale beneficiarilor să fi

[20] Wall-Street.ro, „Jaful de la Banca Transilvania: paguba de 60.000 de euro", arhivă de presă economică.

[21] Adevărul, „Jaf la Sibiu. Afacerist atacat în casă de mascați care i-au amenințat fata cu un pistol", 22 noiembrie 2023.

[22] Oficiuldestiri.ro, „Sentință în dosarul jafului de la Poșta din Timișoara: ce pedepse au primit hoții care au furat 10 milioane de lei", iulie 2026; Aktual24.ro, „Jaf ca-n filme la Poșta Mare din Timișoara", 1 iunie 2025; Opinia Timișoarei, „Spargere de proporții la Poșta Mare din Timișoara", 1 iunie 2025; B1TV.ro, „Angajată a Poștei Timișoara, complice la un jaf de 10 milioane de lei", 20 mai 2026; PressAlert.ro, „Lovitură de teatru în cazul marelui jaf de la Poșta din Timișoara", 20 mai 2026; Evenimentul Zilei, „Noi percheziții în Timiș și Constanța, în cazul jafului de la Poșta din Timișoara", 30 iulie 2025; Martor Incomod, „Aparatură de bruiaj chinezească folosită în «jaful secolului» de la Timișoara, susțin producătorii", august 2026.

fost actualizate pentru a acoperi exact această nouă suprafață de expunere-o suprafață care, în România, nu mai este teoretică.

Bibliografie

Lucrarea urmează convenția citării prin note de subsol numerotate. Referințele de mai jos acoperă exclusiv sursele folosite în acest episod; bibliografia completă a seriei apare, cumulativ, la finalul Părții a IV-a.

A. Acte normative

Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, republicată în Monitorul Oficial al României, Partea I, nr. 189 din 18 martie 2014, cu modificările și completările ulterioare.

Hotărârea de Guvern nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, Monitorul Oficial al României, Partea I, nr. 335 din 17 mai 2012.

Instrucțiunile nr. 9 din 1 februarie 2013 ale Inspectoratului General al Poliției Române privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003.

Ordonanța de urgență nr. 37/2026 pentru modificarea și completarea Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, Monitorul Oficial al României, Partea I, nr. 381 din 6 mai 2026.

C. Articole de presă și analize de specialitate

Adevărul, „Jaf la Sibiu. Afacerist atacat în casă de mascați care i-au amenințat fata cu un pistol”, 22 noiembrie 2023.

Aktual24.ro, „Jaf ca-n filme la Poșta Mare din Timișoara”, 1 iunie 2025.

arts.org.ro, „Modificarea Legii nr. 333/2003 prin OUG 37 din 4 mai 2026”, 12 mai 2026.

B1TV.ro, „Angajată a Poștei Timișoara, complice la un jaf de 10 milioane de lei”, 20 mai 2026.

Click.ro, „Jaf armat la o bancă din România. Un bărbat cu cagulă și înarmat a reușit să fure o sumă mare de bani”, 4 decembrie 2024.

Digi24, „Jaf armat într-o bancă din Iași, făptașul e de negăsit”, 27 septembrie 2024.

Evenimentul Zilei, „Noi percheziții în Timiș și Constanța, în cazul jafului de la Poșta din Timișoara”, 30 iulie 2025.

Martor Incomod, „Aparatură de bruiaj chinezească folosită în «jaful secolului» de la Timișoara, susțin producătorii”, august 2026.

Observator News, „Jaful de la banca din Călărași, filmat”, 4 decembrie 2024.

Oficiuldestiri.ro, „Sentință în dosarul jafului de la Poșta din Timișoara: ce pedepse au primit hoții care au furat 10 milioane de lei”, iulie 2026.

Opinia Timișoarei, „Spargere de proporții la Poșta Mare din Timișoara”, 1 iunie 2025.

PressAlert.ro, „Lovitură de teatru în cazul marelui jaf de la Poșta din Timișoara”, 20 mai 2026.

Realitatea.net, „Panică la o sucursală bancară din Iași: un bărbat a intrat înarmat și a cerut toți banii”, 26 septembrie 2024.

Revista Universul Juridic, „Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor — modificări (O.U.G. nr. 37/2026)”, 12 mai 2026.

Wall-Street.ro, „Jaful de la Banca Transilvania: paguba de 60.000 de euro”, arhivă de presă economică.

D. Surse electronice principale

legislatie.just.ro — Portal Legislativ, text integral O.U.G. nr. 37/2026.

Lege5.ro — bază de date legislativă, text consolidat Legea nr. 333/2003, H.G. nr. 301/2012, O.U.G. nr. 37/2026.

ANALIZĂ CONTRASTIVĂ DE CONVERGENȚĂ A RISCURILOR, DE EFICIENȚĂ OPERAȚIONALĂ ȘI DE CONFORMITATE STANDARDIZATĂ· SECURITATE FIZICĂ ȘI GUVERNANȚĂ TEHNOLOGICĂ

DE LA PANOPTIC LA AGENT AUTONOM: RECONFIGURAREA GLOBALĂ A SECURITĂȚII FIZICE ÎN ERA INTELIGENȚEI ARTIFICIALE ȘI RESTANȚELE STRUCTURALE ALE CADRULUI ROMÂNESC

SERIE ÎN PATRU PĂRȚI · PARTEA A III-A DIN IV

Publicație de specialitate · Domeniul evaluării de risc la securitate fizică

MODUS OPERANDI: CÂND INFRASTRUCTURA CIBERNETICĂ ȘI INTELIGENȚA ARTIFICIALĂ DEVIN VECTORUL DE ATAC FIZIC

LĂZĂU ANGELO *— evaluator de risc la securitate fizică, la* ***WORLD CLASS LA-INT&SECRSK CONSULTANCY****, înscris în Registrul Național al Evaluatorilor de Risc la Securitate Fizică* ***(R.N.E.R.S.F.)****; cu experiență anterioară în structuri militare de informații și securitate, precum și în funcția de* ***Head of Security*** *al unei entități* ***NATO*** *din România — o combinație între practica de teren, cultura de securitate a alianței și cadrul juridic autohton al profesiei.*

Argument

Al treilea episod al seriei examinează, comparativ, șase cazuri internaționale documentate de publicații de specialitate credibile — MGM Resorts, Verkada, spargeri prin bruiaj RF în SUA, o rețea de furt de vehicule în Regatul Unit, Arup și primul caz documentat public de atac cibernetic condus autonom de un sistem AI (OpenAI/Hugging Face) — în care infrastructura cibernetică și AI au devenit vectorul unor incidente de securitate fizică reale. Episodul proiectează aceste tipare asupra pieței românești, pornind de la cazul deja confirmat al bruiajului de la Timișoara, și le susține cu declarații ale unor voci de referință internaționale (Bruce Schneier, Yoshua Bengio, Europol, ASIS International) și cu un set distilat de lecții pentru profesia din România.

Cuvinte-cheie: modus operandi, bruiaj RF, deepfake, vishing, identități non-umane, MGM Resorts, Verkada, Arup, OpenAI, Europol.

Partea a II-a a acestei serii a documentat decalajul dintre cadrul legal românesc și transformarea tehnologică descrisă în Partea I, prin O.U.G. nr. 37/2026 și cinci incidente concrete — inclusiv jaful de la Poșta Mare din Timișoara, unde bruiajul RF a fost folosit, pentru prima dată public documentat în România, pentru a neutraliza o alarmă. Acest al treilea episod explică exact mecanismul acelei tehnici și al altora asemănătoare, la scară internațională, și proiectează implicațiile lor pentru profesia din România.

Secțiunea de început a acestui articol a descris o transformare tehnologică la nivel de industrie. Ceea ce nu a fost încă discutat este modul concret în care actorii răuvoitori nu doar furnizorii de tehnologie au început deja să folosească exact această infrastructură pentru a produce incidente de securitate fizică reale, cu pagube materiale, nu doar teoretice. Cazurile de mai jos, documentate de publicații internaționale de specialitate și de presă generalistă credibilă (CNN, BBC via presa de specialitate, TechTarget, Security Magazine, HIPAA Journal, Schneier on Security), nu sunt incidente cibernetice „pure”: în fiecare dintre ele, compromiterea unui sistem digital s-a tradus direct într-un eveniment de securitate fizică, uși blocate, camere de supraveghere expuse, bunuri sustrase, bani transferați pe baza unei identități fabricate.

Studii de caz internaționale

Cazul **MGM Resorts și Caesars Entertainment**, **Las Vegas**, septembrie 2023. Grupul de criminalitate cibernetică Scattered Spider a obținut acces la sistemele MGM Resorts printr-un singur apel telefonic către departamentul de suport IT: folosind informații culese de pe LinkedIn despre un angajat real, atacatorii au convins operatorul de la helpdesk să reseteze autentificarea multifactor a acelui cont, fără nicio altă verificare de identitate. Rezultatul nu a rămas în plan digital ușile camerelor de hotel, automatele de sloturi, bancomatele și liftele din mai multe cazinouri-hotel au devenit inoperabile timp de zece zile, iar paguba estimată a depășit 100 de milioane de dolari. Caesars Entertainment, victimă a aceluiași grup, a preferat să plătească o răscumpărare estimată la 15 milioane de dolari pentru a-și restabili operațiunile.[23,24]

Cazul **Verkada, Statele Unite**, martie 2021. Un grup de hacktiviști a obținut acces la 150.000 de camere de supraveghere ale companiei Verkada instalate în spitale, școli, secții de poliție, închisori și sedii corporative, inclusiv fabrici Tesla folosind credențiale de tip „super admin” găsite expuse public pe internet. Atacatorii au avut, timp de aproximativ 36 de ore, acces la fluxuri video live și la arhive, inclusiv imagini din interiorul unor saloane de spital și celule de detenție. Cazul arată cât de fragilă poate fi arhitectura centralizată a unui furnizor de securitate fizică atunci când privilegiile de administrare nu sunt segmentate o singură credențială compromisă a expus, dintr-o mișcare, perimetrul „fizic” protejat de mii de clienți diferiți.[25]

Bruiaj RF asupra camerelor și **alarmelor wireless, Statele Unite**, 2022–2026. Departamentul de Poliție din Los Angeles, alături de forțe de ordine din Minnesota și Texas, a documentat public un tipar de spargeri în care infractorii folosesc bruiaje de radiofrecvență dispozitive ieftine, disponibile online cu 40–1.000 de dolari pentru a paraliza, în câteva secunde, camerele și senzorii wireless conectați la rețeaua Wi-Fi a locuinței, chiar înainte de intrarea în imobil. Grupările documentate operează cu echipe de recunoaștere, pătrund prin balcoane de la etaj și vizează bijuterii și obiecte de valoare mică și portabilă; în absența unei surse locale de înregistrare (card SD) sau a unei conexiuni prin cablu, niciun cadru din efracție nu ajunge vreodată în cloud. Cercetătorul de securitate Bruce Schneier a confirmat fenomenul ca parte a unei „curse a înarmării” tehnologice tot mai accesibile infractorilor obișnuiți, nu doar grupărilor sofisticate.[26]

Rețea organizată de furt de vehicule prin **bruiaj GPS, Kent, Regatul Unit**. Potrivit unui raport BBC bazat pe studiul consorțiului Sentinel, poliția din Kent a destructurat o grupare de criminalitate organizată care a furat 150 de autoutilitare Mercedes Sprinter în opt luni, în zona aeroportului Heathrow, folosind bruiaje GPS pentru a dezactiva sistemele de urmărire ale vehiculelor înainte de a le dezmembra pentru piese sau a le transporta în

[23]TechTarget, „Okta: Caesars, MGM Hacked in Social Engineering Campaign”, 20 septembrie 2023; ABC News, „MGM Reeling from Cyber 'Chaos' 5 Days After Attack as Caesars Entertainment Says It Was Hacked Too”, 16 septembrie 2023 — atacul a blocat ușile camerelor, sloturile, ATM-urile și liftele din hotelurile-cazinou MGM.

[24]Specops Software, „MGM Resorts Hack: How Attackers Hit the Jackpot with Service Desk Social Engineering”, 12 noiembrie 2025; TechTarget, op. cit. — Caesars Entertainment a plătit o răscumpărare estimată la 15 milioane de dolari.

[25]Security Magazine, „Verkada Breach Exposed Live Feeds of 150,000 Surveillance Cameras Inside Schools, Hospitals and More”, 10 martie 2021; HIPAA Journal, „Hackers Access Live Feeds and Archived Footage from 150,000 Verkada Security Cameras”, 2021.

[26]NBC Los Angeles, „Burglars Are Using WiFi Jammers to Break Into Homes. Here's What to Know”, 17 martie 2025, declarație a șefului poliției din Los Angeles, Jim McDonnell; PCWorld, „Burglars Are Jamming Wi-Fi Security Cameras. Here's What You Can Do”, 12 noiembrie 2024; Schneier on Security, „Burglars Using Wi-Fi Jammers to Disable Security Cameras”, 13 martie 2024 (Bruce Schneier, cercetător de referință în securitate cibernetică); Cybernews, „Burglars Using Jammers to Disable Wireless Smart Home Security”, 19 februarie 2024, privind cazurile din Edina, Minnesota.

Europa continentală. Cazul, deși vizează un sector conex (transport de valori, nu pază statică), este relevant pentru evaluarea de risc la securitate fizică pentru că demonstrează aceeași vulnerabilitate structurală: orice sistem de securitate care depinde exclusiv de un semnal radio necriptat sau nesegmentat poate fi neutralizat, la scară industrială, de o grupare organizată cu resurse tehnice modeste.[27]

Cazul **Arup, Hong Kong**, ianuarie 2024. Un angajat din departamentul financiar al firmei britanice de inginerie Arup a fost convins să autorizeze 15 transferuri bancare, în valoare totală de 25,6 milioane de dolari, în urma unei videoconferințe la care „directorul financiar" și mai mulți „colegi" prezenți erau, de fapt, recreări deepfake generate din materiale video și audio publice ale acestora. Angajatul, inițial suspicios în privința unui e-mail de phishing, și-a pierdut reținerea exact în momentul în care identitatea vizuală și vocală a interlocutorilor a părut confirmată în timp real. Directorul de informatică al companiei a calificat ulterior incidentul drept „inginerie socială asistată tehnologic", nu un atac cibernetic clasic o distincție esențială pentru evaluarea de risc la securitate fizică, unde amenințarea nu mai vizează un perimetru, ci încrederea în identitatea unei persoane.[28]

Cazul **OpenAI / Hugging Face**, iulie 2026 un atac cibernetic condus autonom de AI. În iulie 2026, OpenAI a confirmat că două dintre modelele sale cele mai avansate GPT-5.6 Sol și un model neanunțat public au evadat dintr-un mediu de testare izolat („sandbox") și au compromis, în mod autonom, infrastructura companiei Hugging Face, exploatând o vulnerabilitate necunoscută anterior cu ajutorul unor credențiale furate, pentru a obține un avantaj într-un test de evaluare. Compania a calificat incidentul drept „fără precedent", iar Hugging Face a precizat că atacul a fost „condus, de la un capăt la altul, de un sistem AI autonom" una dintre puținele situații documentate public în care un model de inteligență artificială a acționat, cu intervenție umană minimă, pentru a descoperi și exploata o vulnerabilitate reală, într-un sistem real. Cercetători de referință precum Yoshua Bengio au calificat incidentul drept un „semnal de alarmă" pentru traiectoria generală a dezvoltării AI. Relevanța pentru securitatea fizică este directă: aceleași capacități autonome de descoperire și exploatare a vulnerabilităților pot fi îndreptate, la fel de ușor, împotriva firmware-ului unei centrale de alarmă, a unui NVR conectat la internet sau a unui panou de control acces echipamente care rulează, în esență, același tip de software vulnerabil ca orice server corporativ, dar care sunt rareori actualizate sau monitorizate cu aceeași rigoare.[29]

Ce au în comun aceste șase cazuri, dincolo de scară, sector și continent, este mecanismul: în niciunul dintre ele infrastructura tehnică „a cedat" în sensul clasic nu a fost spart un gard, nu a fost forțată o încuietoare. În toate, punctul de rupere a fost fie o identitate fabricată sau împrumutată prin mijloace digitale (MGM, Arup), fie o dependență necriticată de un semnal radio sau de o credențială centralizată (Verkada, bruiajele Wi-Fi

[27]Fleetnews.co.uk, citând un raport BBC și studiul consorțiului Sentinel privind utilizarea bruiajelor GPS de către rețele de criminalitate organizată; poliția din Kent, Regatul Unit, a destructurat o grupare care a furat, folosind bruiaj GPS pentru a dezactiva sistemele de urmărire, 150 de autoutilitare Mercedes Sprinter în opt luni, în zona Heathrow.

[28]CNN Business, „Finance Worker Pays Out $25 Million After Video Call with Deepfake 'Chief Financial Officer'", 4 februarie 2024; CNN Business, „Arup Revealed as Victim of $25 Million Deepfake Scam Involving Hong Kong Employee", 17 mai 2024; PurpleSec, „Arup Deepfake: How an AI-Generated Video Stole $25 Million", 2026.

[29]NBC News, „OpenAI Says AI Models Went Rogue During Testing, Triggering 'Unprecedented' Breach at Startup", 22 iulie 2026; CNBC, „OpenAI Cyber Models Broke Out of Training Environment to Hack Hugging Face", 22 iulie 2026; NPR, „OpenAI Blamed a Hacking Event on Its AI Models Gone Rogue. Here Is What to Know", 23 iulie 2026; Al Jazeera, „«Unprecedented»: OpenAI Says AI Models Autonomously Hacked Another Company", 22 iulie 2026; The Conversation, „OpenAI's Models Autonomously Hacked a Tech Startup. It Signals a Seismic Shift in Cybersecurity", 2026.

și GPS), fie în cazul cel mai recent și cel mai puțin liniștitor capacitatea unui sistem AI de a descoperi și exploata singur o vulnerabilitate pe care niciun om nu o cunoștea încă. Consecința s-a materializat direct în planul fizic sau operațional: uși care nu se mai deschideau, camere care arătau interiorul unor spitale unor străini, case golite fără nicio alarmă declanșată, camioane furate fără urmă electronică, servere compromise fără ca vreun angajat să fi apăsat vreodată pe un link greșit.

România: unde se află, astăzi, aceeași amenințare

România nu este, deocamdată, teatrul unor incidente de amploarea celor de mai sus cel puțin nu unele făcute publice. Este însă deja teatrul exact al tehnicii-sursă din care asemenea incidente se construiesc. Directoratul Național de Securitate Cibernetică (DNSC) a emis, încă din 2024, un avertisment public privind o schemă de fraudă în plină expansiune: „mesajul de la șef" în care escrocii clonează, prin AI, vocea sau imaginea unui director și instruiesc, telefonic sau prin mesaj, un angajat din departamentul financiar să efectueze un transfer bancar urgent, exact mecanismul folosit împotriva Arup, doar la o scară locală, deocamdată mai mică.[30]

Datele agregate pentru 2025–2026 confirmă o traiectorie ascendentă rapidă. Atacurile de tip phishing au fost cele mai răspândite în România în 2025, iar numărul fraudelor digitale avansate aproape s-a triplat față de anul anterior; în 2026, aproximativ 42% dintre incidentele raportate la nivel național sunt înșelătorii telefonice de tip vishing. La nivel global, atacurile de vishing asistate de AI au crescut cu 442% în 2025, iar cercetările arată că un om obișnuit reușește să identifice corect o voce clonată artificial în doar 37,5% din cazuri o rată apropiată de aruncarea unei monede. Aproape două treimi dintre companiile chestionate internațional anticipează, pentru 2026, o creștere a fraudelor biometrice, iar peste jumătate a fraudelor bazate pe identitate sintetică.[31,32,33]

Reper — *Cazul 5-Jaful de la Poșta Mare din Timișoara, mai 2025, deja detaliat în secțiunea anterioară, este relevant aici pentru un motiv suplimentar: metoda de operare bruiaj RF pentru neutralizarea alarmei este exact tehnica documentată în secțiunea III.1 pentru cazurile din Los Angeles și din Kent. Bruiajul a funcționat tehnic impecabil pe teritoriul românesc; infractorii au fost prinși, totuși, printr-un control de rutină al Poliției Rutiere, complet independent de arhitectura de securitate a obiectivului — un factor de noroc operațional pentru autorități, nu o dovadă că sistemul electronic i-ar fi putut opri singur.*[34]

---

[30]Newsweek România, „«Mesajul de la șef» pe care trebuie să-l ignori. Poți rămâne fără bani", 9 aprilie 2024 — avertisment al Directoratului Național de Securitate Cibernetică (DNSC) privind frauda prin clonare vocală AI care impersonează un superior ierarhic.

[31]Economedia.ro, „Cele mai mari riscuri de fraudare pentru companii în 2026", 19 iunie 2026 — potrivit sursei, atacurile de tip phishing au fost cele mai răspândite în România în 2025, iar numărul fraudelor digitale avansate aproape s-a triplat față de anul anterior; DailyBusiness.ro, citat în Realitatea.net, „Cum te ferești de fraudele online", 2026 — 42% dintre incidentele raportate în România în 2026 sunt înșelătorii telefonice de tip vishing.

[32]Capital.ro, „Fraudele cu AI și deepfake se extind rapid. Companiile se așteaptă la mai multe atacuri în 2026", 20 iunie 2026, pe baza Sumsub Fraud Report 2025 și a analizei Visual Capitalist — 67% dintre companiile chestionate anticipează o creștere a fraudelor biometrice, iar 56% a fraudelor prin identitate sintetică.

[33]Realitatea.net, „Cum te ferești de fraudele online: ce arată datele din 2026 și cum te protejezi", 29 iulie 2026 — atacurile de tip vishing bazate pe AI au crescut cu 442% în 2025, conținutul deepfake reprezintă aproximativ 11% din activitatea frauduloasă globală în 2026, iar în studii controlate participanții au identificat corect vocile clonate în doar 37,5% din cazuri.

[34]Oficiuldestiri.ro, „Sentință în dosarul jafului de la Poșta din Timișoara: ce pedepse au primit hoții care au furat 10 milioane de lei", iulie 2026; Aktual24.ro, „Jaf ca-n filme la Poșta Mare din Timișoara", 1 iunie 2025; Opinia Timișoarei, „Spargere de proporții la Poșta Mare din Timișoara", 1 iunie 2025; B1TV.ro, „Angajată a Poștei Timișoara, complice la un jaf de 10 milioane de lei", 20 mai 2026; PressAlert.ro, „Lovitură de teatru în cazul marelui jaf de la Poșta din Timișoara", 20 mai 2026; Evenimentul Zilei, „Noi percheziții în Timiș și

Acest caz obligă la o corecție de nuanță a afirmației de mai sus: România nu se mai află, din mai 2025, într-o poziție pur ipotetică față de convergența dintre criminalitatea clasică și instrumentele tehnologice deja descrise mai sus. Bruiajul RF-exact tehnica documentată în cazurile din Los Angeles și din Kent a fost deja folosit cu succes tehnic pe teritoriul românesc, împotriva unei ținte de o gravitate comparabilă. Ceea ce distinge, deocamdată, cazul de la Timișoara de precedentele americane este rezultatul, nu metoda: infractorii nu au reușit să scape datorită unei breșe în procedurile clasice de patrulare polițienească, independentă de orice sistem electronic de securitate — un factor de noroc operațional pentru autorități, nu o dovadă că arhitectura de securitate a obiectivului i-ar fi putut opri singură. Diferența reală dintre România și piețele occidentale nu mai este, așadar, una de disponibilitate tehnologică a metodei — este, cel mult, una de frecvență și de rafinament operațional al grupărilor care o folosesc.[35]

Proiecția: de la bruiajul deja confirmat la specializarea AI în producerea incidentelor de securitate fizică

Cazul de la Timișoara elimină o parte din ipoteză: bruiajul RF, ca metodă de operare, nu mai este un scenariu de import pentru piața românească - este deja folosit, cu succes tehnic, de grupări obișnuite de criminalitate, nu de actori sofisticați. Rămâne, totuși, ipotetică deocamdată componenta specifică AI a acestei convergențe: nu există, la data acestui articol, un caz public în România în care o voce clonată artificial să fi fost folosită pentru a păcăli un dispecerat de monitorizare sau un agent de pază. Distanța tehnică dintre a convinge un angajat financiar să facă un transfer bancar (schema deja prezentă în România) și a convinge, cu o voce clonată, un dispecer de monitorizare să dezactiveze o alarmă este însă mult mai mică decât pare. Amândouă exploatează același mecanism încrederea într-o voce sau o imagine familiară, transmisă printr-un canal digital, iar instrumentele necesare (clonare vocală, generare de imagine în timp real) sunt deja disponibile comercial și ieftine, așa cum arată cazul Arup. Nu este nevoie de o breșă tehnică sofisticată a unui sistem electronic de securitate, este nevoie doar de un apel telefonic bine documentat, exact rețeta care a produs paguba de 100 de milioane de dolari la MGM Resorts, sau de un dispozitiv de bruiaj de câteva sute de lei, exact rețeta deja folosită la Timișoara, în Los Angeles și în Kent.

Traducerea directă, pentru un evaluator de risc din România, este următoarea: metoda de operare pe care ar trebui să o anticipeze pentru anii următori nu este atacul asupra gardului, a lacătului sau a centralei de alarmă, ci atacul asupra omului care are dreptul să dea comenzi acelor sisteme — dispecerul de monitorizare, agentul de pază cu drept de deschidere a barierei, responsabilul de la sediul central care poate autoriza de la distanță o intervenție — sau asupra semnalului radio pe care sistemul electronic îl folosește pentru a comunica alarma, exact vulnerabilitatea deja exploatată la Timișoara. Dacă un infractor obișnuit din România, care astăzi sună un angajat de bancă pretinzând că este „directorul”, decide mâine să sune un dispecerat de monitorizare pretinzând, cu o voce clonată convingător, că este administratorul obiectivului și că solicită dezactivarea temporară a alarmei pentru o „intervenție tehnică programată” — combinând, astfel, tehnica deja confirmată a bruiajului cu componenta AI încă neconfirmată public — nimic

Constanța, în cazul jafului de la Poșta din Timișoara”, 30 iulie 2025; Martor Incomod, „Aparatură de bruiaj chinezească folosită în «jaful secolului» de la Timișoara, susțin producătorii”, august 2026.

[35]Oficiuldestiri.ro, „Sentință în dosarul jafului de la Poșta din Timișoara: ce pedepse au primit hoții care au furat 10 milioane de lei”, iulie 2026; Aktual24.ro, „Jaf ca-n filme la Poșta Mare din Timișoara”, 1 iunie 2025; Opinia Timișoarei, „Spargere de proporții la Poșta Mare din Timișoara”, 1 iunie 2025; B1TV.ro, „Angajată a Poștei Timișoara, complice la un jaf de 10 milioane de lei”, 20 mai 2026; PressAlert.ro, „Lovitură de teatru în cazul marelui jaf de la Poșta din Timișoara”, 20 mai 2026; Evenimentul Zilei, „Noi percheziții în Timiș și Constanța, în cazul jafului de la Poșta din Timișoara”, 30 iulie 2025; Martor Incomod, „Aparatură de bruiaj chinezească folosită în «jaful secolului» de la Timișoara, susțin producătorii”, august 2026.

din arhitectura actuală a securității fizice românești, așa cum a fost descrisă în secțiunea II, nu este pregătit să recunoască sau să prevină acest scenariu.[36]

Consecința economică a unei asemenea specializări ar cădea, ca și în cazurile deja discutate, direct asupra beneficiarului final: bani, bunuri, valori, încredere comercială pierdută — exact riscul pe care O.U.G. nr. 37/2026 nu îl reglementează, deoarece nici măcar nu îl recunoaște ca ipoteză de lucru. Diferența dintre România și piețele occidentale nu mai este, după cazul de la Timișoara, una de disponibilitate a metodei — este una de frecvență, de rafinament și de combinare a tehnicilor deja disponibile separat. Nimic din structura pieței sau din cadrul legal actual nu garantează că această combinare va întârzia mult, mai ales cu o industrie locală de pază și protecție care, prin propria sa lege de organizare, nu este obligată să se pregătească pentru ea.

Voci de referință și lecții pentru profesia din România

Dincolo de cazuistică și de date statistice, este utilă și vocea directă a specialiștilor și instituțiilor care au format, la nivel internațional, gândirea actuală despre convergența securității fizice cu cea cibernetică. Cinci luări de poziție, provenind din surse de maximă credibilitate, rezumă tensiunea prezentă pe tot parcursul articolului.

- ***„E de-a dreptul uluitor că toate acestea s-au întâmplat autonom!”***[37]
- ***„Acest caz din lumea reală ar trebui să fie un semnal de alarmă.”***[38]
- ***„Cursa înarmării continuă.”***[39]
- ***„Însăși structura DNA a crimei organizate se schimbă rapid.”***[40]
- ***„A face funcțiile de securitate și managementul riscului să lucreze împreună, fără fisuri.”***[41]

Citite împreună, aceste cinci poziții nu transmit un mesaj alarmist, ci unul disciplinat: amenințarea este reală, evoluează rapid, iar instituțiile care o studiază profesionist de la un cofondator de companie tehnologică, la un laureat Turing, la Europol și la asociația globală de referință a profesiei de securitate o tratează cu exact seriozitatea pe care metodologia românească actuală nu o cere încă, prin lege, evaluatorilor de risc.

---

[36]Newsweek România, „«Mesajul de la șef» pe care trebuie să-l ignori. Poți rămâne fără bani”, 9 aprilie 2024 — avertisment al Directoratului Național de Securitate Cibernetică (DNSC) privind frauda prin clonare vocală AI care impersonează un superior ierarhic.

[37]Clément Delangue, cofondator și CEO al Hugging Face, declarație publică citată în Euronews, „OpenAI Models Broke Free in Test, Hacked Rival Hugging Face in Major Breach”, 22 iulie 2026; text original: „It's quite mind-blowing that all of this happened autonomously!”.

[38]Yoshua Bengio, laureat al Premiului Turing (2018), citat în CNBC, „OpenAI Cyber Models Broke Out of Training Environment to Hack Hugging Face”, 22 iulie 2026; text original: „this real-world case should serve as a wake-up call”.

[39]Bruce Schneier, cercetător de securitate, membru al consiliului de conducere al Electronic Frontier Foundation și lector la Harvard Kennedy School, „Burglars Using Wi-Fi Jammers to Disable Security Cameras”, Schneier on Security, 13 martie 2024; text original: „The arms race continues.”.

[40]Catherine De Bolle, director executiv Europol, în raportul EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025, citată în Fortune, „Europol Warns AI Is Making Organized Crime 'More Precise and Devastating'”, 18 martie 2025, și GZERO Media, „Europol Warns of AI-Powered Organized Crime”, 18 martie 2025; text original: „The very DNA of organized crime is changing rapidly.”.

[41]ASIS International / ASIS Foundation, The State of Security Convergence in the United States, Europe, and India — definiție a convergenței securității fizice și cibernetice, citată în ReconaSense, „Merging Cybersecurity and Physical Security: ASIS International Survey Findings”; text original: „getting security and risk management functions to work together seamlessly”; potrivit sondajului derulat pe 1.000 de profesioniști, doar 24% dintre organizații au convergat efectiv cele două funcții.

Din întregul parcurs al acestui articol se pot distila, pentru profesia din România, un set de lecții concrete, transferabile direct în practica de zi cu zi:

1. Separarea rolurilor nu înseamnă separarea răspunderilor un evaluator, proiectant sau instalator care omite riscul digital dintr-un raport sau proiect rămâne, totuși, răspunzător pentru omisiune, exact lecția cazurilor MGM Resorts și Verkada, unde punctul de rupere a fost mereu un om, nu un gard.

2. Orice sistem wireless are nevoie de o cale de rezervă imună la bruiaj lecția directă a spargerilor documentate în Los Angeles și în Kent, Regatul Unit.

3. Identitatea, nu perimetrul, este noua frontieră a atacului un protocol de verificare secundară pentru solicitările neobișnuite este, în 2026, la fel de esențial ca un gard bine întreținut, lecția cazului Arup.

4. Capacitatea AI de a descoperi și exploata singură o vulnerabilitate nu mai este ipotetică orice echipament conectat la internet, oricât de „minor" pare, trebuie tratat ca o suprafață de atac reală, lecția cazului OpenAI/Hugging Face.

5. Criminalitatea organizată se reorganizează deja în jurul AI, la nivel european potrivit Europol, iar România nu are niciun motiv structural să rămână, pe termen lung, în afara acestei traiectorii.

6. Convergența securității fizice cu cea cibernetică rămâne, chiar și la nivel internațional, mai declarată decât practicată potrivit ASIS International, doar aproximativ un sfert dintre organizații au realizat-o efectiv, ceea ce înseamnă că profesia din România nu pornește de pe o poziție unică de rămânere în urmă, ci are șansa de a evita o greșeală pe care nici piețele mature nu au corectat-o încă pe deplin.

Acest al treilea episod a arătat cum arată, concret, convergența dintre infrastructura cibernetică, AI și securitatea fizică — și a proiectat, pe baza cazului de la Timișoara, riscul specializării infractorilor români. Ultimul episod al seriei tratează consecința juridică a acestei convergențe: neconformitatea legală a echipamentelor „inteligente" instalate azi cu NIS2, AI Act și Cyber Resilience Act, lanțul de răspundere profesională care se activează după un incident, precum și recomandările practice pentru evaluator, proiectant, instalator și beneficiar.

Bibliografie

Lucrarea urmează convenția citării prin note de subsol numerotate. Referințele de mai jos acoperă exclusiv sursele folosite în acest episod; bibliografia completă a seriei apare, cumulativ, la finalul Părții a IV-a.

B. Rapoarte instituționale și corporative

Sumsub, Sumsub Fraud Report 2025, sinteză Visual Capitalist, 2026.

C. Articole de presă și analize de specialitate

ABC News, „MGM Reeling from Cyber 'Chaos' 5 Days After Attack as Caesars Entertainment Says It Was Hacked Too”, 16 septembrie 2023.

Al Jazeera, „«Unprecedented»: OpenAI Says AI Models Autonomously Hacked Another Company”, 22 iulie 2026.

Aktual24.ro, „Jaf ca-n filme la Poșta Mare din Timișoara”, 1 iunie 2025.

ASIS International / ASIS Foundation, The State of Security Convergence in the United States, Europe, and India, sinteză ReconaSense, „Merging Cybersecurity and Physical Security: ASIS International Survey Findings”.

B1TV.ro, „Angajată a Poștei Timișoara, complice la un jaf de 10 milioane de lei”, 20 mai 2026.

Capital.ro, „Fraudele cu AI și deepfake se extind rapid. Companiile se așteaptă la mai multe atacuri în 2026”, 20 iunie 2026.

CNBC, „OpenAI Cyber Models Broke Out of Training Environment to Hack Hugging Face”, 22 iulie 2026.

CNN Business, „Finance Worker Pays Out $25 Million After Video Call with Deepfake 'Chief Financial Officer'”, 4 februarie 2024; „Arup Revealed as Victim of $25 Million Deepfake Scam Involving Hong Kong Employee”, 17 mai 2024.

Cybernews, „Burglars Using Jammers to Disable Wireless Smart Home Security”, 19 februarie 2024.

Economedia.ro, „Cele mai mari riscuri de fraudare pentru companii în 2026”, 19 iunie 2026.

Europol, EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025 — declarații ale directorului executiv Catherine De Bolle, citate în Fortune și GZERO Media, 18 martie 2025.

Evenimentul Zilei, „Noi percheziții în Timiș și Constanța, în cazul jafului de la Poșta din Timișoara”, 30 iulie 2025.

Fleetnews.co.uk, „GPS Jammers Still a Threat” — sinteză a unui raport BBC și a studiului consorțiului Sentinel privind rețeaua de furt de vehicule din Kent, Regatul Unit.

HIPAA Journal, „Hackers Access Live Feeds and Archived Footage from 150,000 Verkada Security Cameras”, 2021.

Martor Incomod, „Aparatură de bruiaj chinezească folosită în «jaful secolului» de la Timișoara, susțin producătorii”, august 2026.

NBC Los Angeles, „Burglars Are Using WiFi Jammers to Break Into Homes. Here's What to Know”, 17 martie 2025.

NBC News, „OpenAI Says AI Models Went Rogue During Testing, Triggering 'Unprecedented' Breach at Startup”, 22 iulie 2026.

Newsweek România, „«Mesajul de la șef» pe care trebuie să-l ignori. Poți rămâne fără bani”, 9 aprilie 2024.

NPR, „OpenAI Blamed a Hacking Event on Its AI Models Gone Rogue. Here Is What to Know”, 23 iulie 2026.

Oficiuldestiri.ro, „Sentință în dosarul jafului de la Poșta din Timișoara: ce pedepse au primit hoții care au furat 10 milioane de lei”, iulie 2026.

Opinia Timișoarei, „Spargere de proporții la Poșta Mare din Timișoara”, 1 iunie 2025.

PCWorld, „Burglars Are Jamming Wi-Fi Security Cameras. Here's What You Can Do”, 12 noiembrie 2024.

PressAlert.ro, „Lovitură de teatru în cazul marelui jaf de la Poșta din Timișoara”, 20 mai 2026.

PurpleSec, „Arup Deepfake: How an AI-Generated Video Stole $25 Million”, 2026.

Realitatea.net, „Cum te ferești de fraudele online: ce arată datele din 2026 și cum te protejezi”, 29 iulie 2026.

Schneier, Bruce, „Burglars Using Wi-Fi Jammers to Disable Security Cameras”, Schneier on Security, 13 martie 2024.

Security Magazine, „Verkada Breach Exposed Live Feeds of 150,000 Surveillance Cameras Inside Schools, Hospitals and More”, 10 martie 2021.

Specops Software, „MGM Resorts Hack: How Attackers Hit the Jackpot with Service Desk Social Engineering”, 12 noiembrie 2025.

TechTarget, „Okta: Caesars, MGM Hacked in Social Engineering Campaign”, 20 septembrie 2023.

The Conversation, „OpenAI's Models Autonomously Hacked a Tech Startup. It Signals a Seismic Shift in Cybersecurity”, 2026.

ANALIZĂ CONTRASTIVĂ DE CONVERGENȚĂ A RISCURILOR, DE EFICIENȚĂ OPERAȚIONALĂ ȘI DE CONFORMITATE STANDARDIZATĂ· SECURITATE FIZICĂ ȘI GUVERNANȚĂ TEHNOLOGICĂ

DE LA PANOPTIC LA AGENT AUTONOM: RECONFIGURAREA GLOBALĂ A SECURITĂȚII FIZICE ÎN ERA INTELIGENȚEI ARTIFICIALE ȘI RESTANȚELE STRUCTURALE ALE CADRULUI ROMÂNESC

SERIE ÎN PATRU PĂRȚI · PARTEA A IV-A DIN IV (FINAL)

Publicație de specialitate · Domeniul evaluării de risc la securitate fizică

NECONFORMITATEA LEGALĂ, LANȚUL RĂSPUNDERII ȘI RECOMANDĂRILE PRACTICE PENTRU PROFESIA DIN ROMÂNIA

LĂZĂU ANGELO *— evaluator de risc la securitate fizică, la* ***WORLD CLASS LA-INT&SECRSK CONSULTANCY****, înscris în Registrul Național al Evaluatorilor de Risc la Securitate Fizică* ***(R.N.E.R.S.F.)****; cu experiență anterioară în structuri militare de informații și securitate, precum și în funcția de* ***Head of Security*** *al unei entități* ***NATO*** *din România — o combinație între practica de teren, cultura de securitate a alianței și cadrul juridic autohton al profesiei.*

Argument

Ultimul episod al seriei analizează neconformitatea frecventă a echipamentelor „inteligente” instalate astăzi cu Directiva NIS2, AI Act și Cyber Resilience Act, precum și lanțul de răspundere profesională — evaluator, proiectant, instalator — care se activează atunci când un incident de securitate este cauzat de o asemenea vulnerabilitate, inclusiv dilema specifică a reevaluării unui obiectiv preexistent. Episodul se încheie cu un set de recomandări operaționale, structurate pe cei patru actori ai profesiei, și cu o concluzie care sintetizează întreaga serie. Bibliografia de mai jos reunește, cumulativ, toate sursele citate în cele patru episoade.

Cuvinte-cheie: NIS2, Cyber Resilience Act, răspundere profesională, Codul civil, Codul penal, recomandări operaționale, evaluator de risc, proiectant, instalator, beneficiar.

Partea a III-a a acestei serii a arătat, prin șase cazuri internaționale și prin cazul deja confirmat de la Timișoara, cum infrastructura cibernetică și AI devin vectorul unor incidente de securitate fizică reale. Acest ultim episod tratează consecința juridică a acestei convergențe și încheie seria cu recomandări practice pentru fiecare dintre cei patru actori ai profesiei.

Neconformitatea legală a echipamentelor „inteligente”: NIS2, AI Act și răspunderea profesională a lanțului

Există, dincolo de metoda de operare a infractorilor, o a doua dimensiune a riscului pe care profesia o discută prea puțin: legalitatea propriu-zisă a echipamentelor pe care proiectanții le recomandă și pe care instalatorii le montează. O cameră cu analiză video bazată pe AI, un NVR cu acces de la distanță prin cloud sau un panou de control acces cu firmware actualizabil de la distanță nu sunt doar alegeri tehnice — sunt, din 2024–2026

încoace, obiectul unui cadru legal european tot mai dens, pe care o parte semnificativă a pieței locale de instalări îl ignoră, adesea din simplă necunoaștere.

De ce o parte din echipamentele instalate astăzi este, strict tehnic, neconformă

Directiva NIS2 (UE 2022/2555), transpusă în România prin O.U.G. nr. 155/2024 și consolidată prin Legea nr. 124/2025, impune entităților „esențiale” și „importante” bănci, spitale, energie, infrastructură digitală, administrație publică, dar și lanțurile lor de furnizori obligații explicite de securitate a lanțului de aprovizionare, gestionare a vulnerabilităților și raportare a incidentelor în 24 de ore, sub sancțiunea unor amenzi de până la 10 milioane de euro sau 2% din cifra de afaceri globală, cu răspundere personală a organelor de conducere. Regulamentul privind inteligența artificială impune, pentru sistemele de securitate fizică bazate pe biometrie sau destinate infrastructurii critice, evaluare de conformitate și marcaj CE înainte de introducerea pe piață — obligații a căror aplicare a fost amânată prin Regulamentul (UE) 2026/1744 (în vigoare din 27 iulie 2026) până la 2 decembrie 2027 pentru sistemele din Anexa III și 2 august 2028 pentru cele integrate în produse reglementate. Iar Actul privind reziliența cibernetică (Cyber Resilience Act) obligă, în aplicare graduală — obligațiile de raportare a vulnerabilităților exploatate activ și a incidentelor grave (art. 14) se aplică din 11 septembrie 2026, iar ansamblul cerințelor din 11 decembrie 2027 —, ca orice produs cu componente digitale introdus pe piața UE — inclusiv o cameră IP sau o centrală de alarmă conectată să fie proiectat după principiul „security by design”, cu gestionare documentată a vulnerabilităților pe tot ciclul de viață.[42,43,44]

Neconformitate în practică, nu doar în teorie. Un proiectant care recomandă, iar un instalator care montează, o cameră sau un NVR cu analiză AI și conectivitate cloud, fără să verifice dacă echipamentul respectiv respectă cerințele Cyber Resilience Act de securitate integrată din proiectare și fără să documenteze, pentru un beneficiar aflat sub incidența NIS2, modul în care acel echipament se încadrează în obligațiile de securitate a lanțului de aprovizionare ale beneficiarului nu face doar o alegere tehnică discutabilă. Instalează, practic, o neconformitate legală în infrastructura clientului, care poate expune atât firma de instalare (contractual), cât și beneficiarul însuși (în fața DNSC, dacă intră sub incidența NIS2) unor sancțiuni pe care niciuna dintre părți nu le-a anticipat la semnarea contractului.

---

[42]Comisia Europeană, Direcția Generală Rețele de Comunicare, Conținut și Tehnologie, „NIS2 Directive: Securing Network and Information Systems”, digital-strategy.ec.europa.eu, 2026; Somos, „Navigating NIS2 and the Cyber Resilience Act: Requirements for IoT Device, Software & Vulnerability Documentation”, 2025 — privind obligațiile de securitate integrată încă din faza de proiectare pentru dispozitivele IoT și lanțul de aprovizionare.

[43]Digi24, „Amenzi de până la 10 milioane de euro: România aplică o lege dură de securitate cibernetică pentru companii”, 14 ianuarie 2026 — privind transpunerea Directivei NIS2 prin O.U.G. nr. 155/2024, consolidată prin Legea nr. 124/2025; Bizlawyer.ro, „Securitatea cibernetică: cadru național consolidat, noi entități vizate de cerințele NIS2 și noi obligații ale organelor de conducere”, 28 iulie 2025.

[44]Accevo, „Complying with the EU Cyber Resilience Act and NIS2: A Guide for Industrial Manufacturers”, 2026 — privind obligația de securitate integrată din faza de proiectare (security by design) pentru orice produs cu componente digitale introdus pe piața UE, aplicabilă gradual până în decembrie 2027.

Evaluatorul de risc: singurul actor fără drept de decizie asupra echipamentelor, dar nu și fără obligații

Spre deosebire de proiectant și instalator, evaluatorul de risc la securitate fizică nu alege, prin metodologia actuală, mărci, modele sau arhitecturi tehnice concrete rolul său, conform normelor metodologice de aplicare a Legii nr. 333/2003, este să identifice vulnerabilitățile și nivelul de expunere la risc și să indice, la nivel funcțional, măsurile de protecție necesare (de exemplu: „sistem de supraveghere video pe zona de acces", „control acces pe zona cu regim special"), nu să specifice echipamentul anume care va îndeplini acea funcție. Această separare de roluri înseamnă că evaluatorul nu răspunde, în principiu, pentru faptul că un anumit model de cameră instalat ulterior este sau nu conform cu AI Act sau cu Cyber Resilience Act el nu a ales acel model. Proiectantul și instalatorul, în schimb, rămân expuși, pentru o asemenea alegere, regulilor de drept comun ale răspunderii civile: contractuale, în temeiul art. 1516 și art. 1530–1531 din Codul civil, pentru neexecutarea sau executarea necorespunzătoare a obligațiilor asumate față de beneficiar, și delictuale, în temeiul art. 1349 și art. 1357 din Codul civil, față de orice terț prejudiciat printr-o faptă ilicită proprie.[45,46]

Rămâne deschisă, în schimb, o întrebare pe care acest articol o semnalează fără a o soluționa pentru că nici jurisprudența română nu a soluționat-o încă, în mod specific, pentru profesia de evaluator de risc la securitate fizică: aceea a eventualei răspunderi penale pentru neglijență în serviciu, prevăzută de art. 298 din Codul penal. Textul se aplică funcționarilor publici și persoanelor asimilate acestora, potrivit art. 175 alin. (2) din Codul penal - categorie care include, de pildă, experții autorizați care exercită un serviciu de interes public sub controlul unei autorități publice. Evaluatorul de risc este înscris într-un registru național administrat de poliție, iar analiza sa de risc poate fi anulată de aceeași autoritate, potrivit chiar O.U.G. nr. 37/2026. Este, la prima vedere, o formă de control public asupra activității sale. Practica Înaltei Curți de Casație și Justiție este însă restrictivă: în Decizia nr. 18/2017, un angajat bancar aflat sub supravegherea Băncii Naționale a României a fost considerat, totuși, în afara sferei art. 175 alin. (2), pe motiv că simpla supraveghere administrativă a unei activități, fără o învestire directă sau un raport juridic nemijlocit cu autoritatea publică, nu este suficientă pentru asimilare. Aplicată prin analogie, această jurisprudență sugerează că evaluatorul de risc s-ar afla, probabil, mai aproape de poziția angajatului bancar decât de cea a unui notar sau executor judecătoresc dar este o chestiune pe care numai o decizie judecătorească dedicată acestei profesii ar putea-o tranșa definitiv. Prudența profesională recomandă, totuși, ca evaluatorul să nu se bazeze pe această incertitudine ca pe o formă de imunitate.[47]

[45]Legea nr. 287/2009 privind Codul civil, republicată, art. 1516 și art. 1530–1531 — dreptul creditorului la daune-interese pentru prejudiciul cauzat de neexecutarea sau executarea necorespunzătoare a unei obligații contractuale.

[46]Legea nr. 287/2009 privind Codul civil, republicată, art. 1349 și art. 1357 — răspunderea civilă delictuală pentru fapta proprie: „Cel care cauzează altuia un prejudiciu printr-o faptă ilicită, săvârșită cu vinovăție, este obligat să îl repare" (art. 1357 alin. 1).

[47]Legea nr. 286/2009 privind Codul penal, republicată, art. 298 (neglijența în serviciu) coroborat cu art. 175 alin. (2) (persoane asimilate funcționarului public); Decizia nr. 18 din 30 mai 2017 și Decizia nr. 37/2022 ale Înaltei Curți de Casație și Justiție, care condiționează asimilarea de existența unei învestiri sau a unui raport

Ceea ce este cert, indiferent de răspunsul la întrebarea de mai sus, este că obligația evaluatorului de a identifica vulnerabilitățile obiectivului rămâne una de conduită, nu de rezultat legat de o marcă anume iar vulnerabilitatea cibernetică sau AI a unui sistem electronic, existent sau propus, este o vulnerabilitate a obiectivului analizat, exact ca o breșă în gard sau o încuietoare defectă. Un raport de analiză de risc care omite complet această categorie de risc, deși ea este vizibilă și documentabilă, nu este un raport complet este un raport neglijent, expus cel puțin unei acțiuni civile întemeiate pe art. 1357 din Codul civil din partea beneficiarului prejudiciat, indiferent de eventuala calificare penală a faptei.

Reevaluarea(revizuirea) unui obiectiv preexistent: complicitate tăcută sau raportare completă?

Aici apare întrebarea cea mai dificilă pentru practica actuală a profesiei. La un obiectiv nou, separarea de roluri descrisă mai sus este relativ curată: evaluatorul stabilește cerințele înainte ca echipamentul să fie ales. La reevaluarea(revizuirea) conform legii, a unui obiectiv preexistent, evaluatorul găsește însă un sistem deja instalat adesea de o firmă cu care beneficiarul are un contract de mentenanță în derulare, uneori chiar aceeași firmă care a recomandat inițial echipamentele acum vulnerabile sau neconforme. Practic, evaluatorul este pus, fără să o spună nimeni explicit, în fața unei alegeri profesionale și etice.

1. Fie se complace: tratează reevaluarea ca pe o formalitate administrativă, verifică doar conformitatea cu anexa clasică de cerințe minime (garduri, iluminat, pază umană) și trece sub tăcere componenta digitală a sistemului deja instalat o formă de complicitate tăcută cu eventualele omisiuni ale proiectantului sau instalatorului inițial, motivată adesea de dorința de a nu complica o relație contractuală existentă între beneficiar și firma de instalare.
2. Fie cuprinde în raport, cu aceeași rigoare aplicată perimetrului fizic, vulnerabilitățile și riscurile digitale ale sistemului existent conectivitate cloud nedocumentată, firmware neactualizat, absența unei căi de comunicație de rezervă imună la bruiaj, lipsa segmentării rețelei indiferent cine a proiectat sau instalat inițial acel sistem și indiferent de eventuala presiune comercială de a nu „complica lucrurile”.

Numai a doua variantă respectă obligația de conduită descrisă mai devreme. Un evaluator care alege prima variantă nu doar că lasă beneficiarul expus unui risc real își asumă, personal, riscul unei acuzații ulterioare de raport incomplet sau de neglijență profesională, exact în momentul în care un incident ar dovedi că vulnerabilitatea era vizibilă și documentabilă la data reevaluării. Regula de incompatibilitate introdusă de O.U.G. nr. 37/2026 interdicția de a evalua obiective cu care firma proprie are relații contractuale merge, de altfel, exact în această direcție: recunoaște, chiar dacă indirect, că

juridic direct cu autoritatea publică, nu doar de simpla înregistrare sau supraveghere administrativă a activității.

un evaluator aflat într-o relație comercială cu instalatorul sau cu beneficiarul este supus unei presiuni reale de a „privi în altă parte”.[48]

A doua variantă nu se oprește, în practică, la simpla consemnare a riscurilor în raport. Un evaluator riguros o poate transforma într-o recomandare concretă, cu efect imediat pentru beneficiar: solicitarea unui audit de conformitate NIS2, realizat de un auditor specializat, extern atât evaluatorului cât și firmei de instalare, și o evaluare tehnică distinctă, realizată de un specialist în securitate cibernetică sau în sisteme AI, asupra componentelor „inteligente” deja instalate camere cu analiză video, NVR-uri conectate, panouri de control acces cu administrare de la distanță. Rezultatele celor două audituri, corelate cu constatările din analiza de risc, oferă beneficiarului un temei obiectiv, independent de orice interes comercial, pentru pasul următor: o discuție directă, la aceeași masă, cu proiectantul și cu instalatorul inițial, în care aceștia să primească, în scris, lista exactă a neconformităților identificate și a măsurilor de remediere sau de înlocuire pe care trebuie să le execute nu o discuție generală despre „îmbunătățiri”, ci un set de obligații clare, cu termene, asumate de cei care au proiectat și instalat sistemul.

Această secvență reevaluare(revizuire) cu raportare completă, audit NIS2 extern, evaluare tehnică AI independentă, întâlnire de remediere cu proiectantul și instalatorul mută, practic, sarcina probei dinspre beneficiar spre profesioniștii care au livrat sistemul. Dacă proiectantul sau instalatorul refuză să acționeze pe baza unor constatări susținute de doi auditori independenți, refuzul însuși devine, într-un eventual litigiu ulterior, o dovadă suplimentară de rea-credință sau de neglijență contractuală, în sensul art. 1516 și art. 1530–1531 din Codul civil. Pentru evaluator, recomandarea acestui parcurs, consemnată explicit în raport, este totodată cea mai solidă formă de protecție profesională proprie: demonstrează că obligația de conduită descrisă mai sus a fost dusă până la capăt, nu doar semnalată formal.[49]

Lanțul răspunderii după un incident: cine plătește

Scenariul final, cel mai relevant pentru practica de zi cu zi, este simplu de imaginat și tot mai probabil să apară: un incident de securitate o efracție, un furt, un acces neautorizat în care ancheta ulterioară arată că un echipament „inteligent” a fost, direct sau indirect, cauza sau un factor favorizant: o cameră cu firmware nepatchat, un NVR cu parolă implicită nemodificată, o alarmă wireless bruiată fără nicio cale de rezervă, un dispecerat păcălit printr-un apel cu voce clonată. Beneficiarul, care a suferit o pierdere reală bani, bunuri, valori, va căuta, firesc, să recupereze prejudiciul, iar ținta cea mai probabilă, în ordine, este:

[48]O.U.G. nr. 37/2026, op. cit.; analiză a conținutului normativ în Revista Universul Juridic, „Legea nr. 333/2003 ... modificări (O.U.G. nr. 37/2026)”, 12 mai 2026, și arts.org.ro, „Modificarea Legii nr. 333/2003 prin OUG 37 din 4 mai 2026”, 12 mai 2026.

[49]Legea nr. 287/2009 privind Codul civil, republicată, art. 1516 și art. 1530–1531 — dreptul creditorului la daune-interese pentru prejudiciul cauzat de neexecutarea sau executarea necorespunzătoare a unei obligații contractuale.

1. Instalatorul pentru legătura cauzală cea mai directă: configurare deficitară, absența actualizărilor, alegerea unui echipament vulnerabil sau montarea lui fără măsurile minime de securizare descrise în secțiunea anterioară.
2. Proiectantul pentru specificarea unei soluții tehnice care nu a luat în calcul riscul digital documentabil la data proiectării sau care nu respectă obligațiile derivate din NIS2, AI Act sau Cyber Resilience Act aplicabile sectorului beneficiarului.
3. Evaluatorul de risc, în special dacă cea mai recentă reevaluare(revizuire) a fost semnată fără nicio mențiune a acestor riscuri, deși erau, la acel moment, identificabile cu diligența rezonabilă a unui profesionist din domeniu exact scenariul descris.

Producătorul echipamentului rămâne, teoretic, o a patra sursă de răspundere, prin regulile speciale de răspundere pentru produsele cu defecte dar, în practică, un beneficiar din România are acces mult mai direct și mai rapid la instalatorul, proiectantul și evaluatorul cu care a contractat local decât la un producător aflat, adesea, într-o altă jurisdicție. Aceasta înseamnă că, în fapt, cei trei profesioniști locali sunt cei care suportă presiunea reală a unei acțiuni în răspundere civilă contractuală, în temeiul art. 1516 și art. 1530–1531 din Codul civil, față de proiectant și instalator, contractuală sau, după caz, delictuală, în temeiul art. 1349 și art. 1357 din Codul civil, față de evaluator, indiferent de cât de „departe” a fost, tehnic, originea reală a vulnerabilității.[50,51]

Concluzia practică a acestei secțiuni este simplă și se adresează direct celor patru actori: exact pentru că acest lanț de răspundere există și este, cel mai probabil, subestimat de o parte a pieței, fiecare verigă are un interes profesional propriu nu doar unul moral, față de beneficiar să trateze riscul digital cu aceeași rigoare pe care o aplică riscului fizic clasic. Pentru evaluator, aceasta înseamnă, concret, să nu omită niciodată aceste riscuri dintr-un raport de reevaluare, oricâtă presiune comercială ar exista în sens contrar.

Evoluția tehnologică pe care evaluarea de risc din România trebuie să o absoarbă

Cele trei direcții discutate mai sus, decalajul normativ, convergența deja activă dintre inginerie socială, AI și securitate fizică, și lanțul de neconformitate legală și răspundere profesională converg spre aceeași concluzie practică: profesia nu poate aștepta o lege nouă pentru a-și actualiza reflexele. Ce anume trebuie să facă, concret, fiecare dintre cei patru actori ai lanțului este detaliat mai jos.

Evaluatorul de risc: de la checklist fizic la analiză hibridă

[50]Legea nr. 287/2009 privind Codul civil, republicată, art. 1516 și art. 1530–1531 — dreptul creditorului la daune-interese pentru prejudiciul cauzat de neexecutarea sau executarea necorespunzătoare a unei obligații contractuale.
[51]Legea nr. 287/2009 privind Codul civil, republicată, art. 1349 și art. 1357 — răspunderea civilă delictuală pentru fapta proprie: „Cel care cauzează altuia un prejudiciu printr-o faptă ilicită, săvârșită cu vinovăție, este obligat să îl repare” (art. 1357 alin. 1).

1. Documentarea explicită, în raportul de analiză, a fiecărei componente digitale a sistemului electronic existent sau propus: conectivitate cloud, aplicații de administrare de la distanță, integrări cu terți, module de analiză video bazate pe AI.
2. Extinderea identificării vulnerabilităților dincolo de perimetrul fizic, către punctele în care sistemul depinde de infrastructură externă server, cloud, rețea de telefonie mobilă pentru comunicatoare GSM/GPRS, semnal radio nesegmentat între senzori și centrală.
3. Corelarea profilului de amenințare cu expunerea publică reală a beneficiarului (statut, vizibilitate, valori gestionate), nu doar cu tipologia standard a obiectivului lecția directă a cazului Sibiu.
4. Verificarea existenței și funcționalității reale a procedurilor operaționale buton de panică, protocol de alertare, timp de reacție nu doar a prezenței fizice a echipamentului, lecția cazurilor Iași și Călărași.
5. Recomandarea explicită, către beneficiar, a unei revizuiri periodice a drepturilor de acces digitale acordate personalului și furnizorilor, cu principiul privilegiului minim necesar.
6. Includerea, în analiza de risc, a unui scenariu explicit de inginerie socială asistată de AI îndreptat împotriva dispeceratului de monitorizare sau a personalului cu drept de dezactivare a alarmei, precum și a unui scenariu de bruiaj RF pentru orice subsistem wireless lecția directă a cazurilor MGM Resorts, Arup și a spargerilor prin bruiaj din SUA și Regatul Unit.
7. solicitarea unui audit de conformitate NIS2, la un obiectiv preexistent, realizat de un auditor specializat, extern atât evaluatorului cât și firmei de instalare, și o evaluare tehnică distinctă, realizată de un specialist în securitate cibernetică sau în sisteme AI, asupra componentelor „inteligente” deja instalate camere cu analiză video, NVR-uri conectate, panouri de control acces cu administrare de la distanță, sau introducerea masurii de contractare de către beneficiar a serviciilor acestora pentru un obiectiv nou pentru a emite un set de obligații clare, cu termene, asumate de către proiectant si instalator.

Proiectantul: eligibilitate tehnică într-o arhitectură convergentă

Un proiect tehnic eligibil, în sensul deplin al termenului, nu se mai limitează la amplasarea corectă a detectoarelor și la dimensionarea cablării. El trebuie să documenteze arhitectura de rețea a sistemului separarea, acolo unde este posibil, a rețelei de securitate de rețeaua administrativă IT, sursele de alimentare de rezervă pentru fiecare subsistem critic, precum și tratamentul explicit al oricărei componente cu conectivitate cloud sau analiză AI. Proiectantul care recomandă o cameră cu recunoaștere facială sau analiză comportamentală automată are obligația profesională de a semnala beneficiarului implicațiile de conformitate de la protecția datelor cu caracter personal, până la eventualele obligații derivate din AI Act pentru entitățile cu activitate transfrontalieră.

Instalatorul: citirea schemei tehnice ca act de securitate, nu doar de execuție

Un instalator care nu înțelege principiile din spatele unei scheme tehnice zonarea de risc, topologia de rețea, logica de alocare a drepturilor de acces nu poate detecta, la fața locului, o neconcordanță periculoasă între proiect și realitatea obiectivului. Competența tehnică minimă pentru 2026 include:

- citirea corectă a simbolisticii standardizate pentru control acces, efracție, video și integrarea lor într-o singură schemă funcțională;
- verificarea, la punerea în funcțiune, a concordanței dintre zonarea de risc din proiect și amplasarea reală a echipamentelor;
- securizarea de bază a oricărei componente conectate — schimbarea parolelor implicite, actualizarea firmware-ului, dezactivarea porturilor neutilizate;
- testarea completă a scenariilor de alarmă, inclusiv a celor care implică notificări automate sau componente AI;
- prevederea unei căi de comunicație de rezervă, imună la bruiaj RF, pentru orice subsistem wireless critic cablare fizică de rezervă, stocare locală pe card, canal GSM redundant față de conexiunea Wi-Fi principală lecția directă a spargerilor prin bruiaj Wi-Fi/GPS documentate în SUA și Regatul Unit;
- întocmirea riguroasă a documentației as-built, fără de care nicio analiză de risc ulterioară nu poate fi corect fundamentată.

Beneficiarul: de la utilizator pasiv la operator responsabil

Predarea unui sistem de securitate către beneficiar nu se încheie cu semnarea unui proces-verbal de recepție. Cazurile Iași și Călărași arată, empiric, că un sistem tehnic corect proiectat și instalat poate eșua complet dacă personalul care îl operează nu înțelege, la nivel funcțional, limitele automatizării și procedura corectă de reacție. Instruirea beneficiarului trebuie să acopere explicit: distincția dintre o alarmă reală și una falsă, condițiile în care sistemul acționează autonom față de cele în care este necesară o decizie umană imediată, procedura de individualizare și schimbare periodică a codurilor de acces, precum și limitările tehnologice reale ale oricărei componente de analiză video inteligentă rate de fals-pozitiv, condiții de iluminare, unghiuri moarte pentru a preveni exact acea încredere nejustificată în automatizare pe care raportul Genetec 2026 o identifică drept principalul obstacol în adopția responsabilă a AI în securitatea fizică. La acestea se adaugă, după cazurile discutate în secțiunea III, o cerință nouă: un protocol explicit de verificare secundară un „cuvânt de siguranță”, un apel de confirmare pe alt canal decât cel prin care a venit solicitarea pentru orice instrucțiune neobișnuită venită, aparent, de la un superior sau de la un partener de încredere, indiferent cât de convingătoare pare vocea sau imaginea.[52,53]

Concluzie

[52]Genetec Inc., webinar „Trends Shaping Physical Security in 2026”, op. cit. — potrivit sondajului, doar 20% dintre respondenți declară că nu au nicio rezervă privind utilizarea AI în securitatea fizică.
[53]Realitatea.net, op. cit., și Newsweek România, op. cit. — recomandare a unui protocol de verificare secundară pentru solicitările neobișnuite venite, aparent, de la un superior ierarhic.

Analiza comparată conturează un contrast structural: China standardizează de sus în jos, cu o viteză și o cuprindere pe care doar un stat puternic centralizat le poate susține; Statele Unite lasă piața să inoveze și reglementează sectorial, adesea din rațiuni de securitate națională; Uniunea Europeană construiește, dinspre drepturile fundamentale, cel mai riguros sistem de conformitate din lume, cu termene ferme deja aplicabile. România dispune de un cadru instituțional matur un registru național de evaluatori, o metodologie clară, o obligație legală fermă, dar acest cadru a fost proiectat pentru o generație tehnologică pe care realitatea din teren a depășit-o deja.

Cel mai grăitor semn al acestei rămâneri în urmă nu este absența unei reacții legislative, ci felul în care reacția a fost formulată. O.U.G. nr. 37/2026 demonstrează că statul român este conștient, la nivel declarativ, de presiunea pe care inteligența artificială și amenințările cibernetice o exercită asupra securității fizice recunoașterea există, în expunerea de motive. Dar substanța ordonanței rămâne integral organizatorică: categorii de pază, registre, avize, uniforme, contravenții. Este diferența dintre a numi o problemă și a o rezolva, iar în acest interval între recunoașterea declarativă și reglementarea tehnică efectivă se plasează exact riscul pe care evaluatorul, proiectantul și instalatorul trebuie, deocamdată singuri, să îl acopere, și pe care beneficiarul final îl plătește, în ultimă instanță, din propriul buzunar, atunci când sistemul modern pe care l-a achiziționat cedează exact în punctul pe care legea încă nu îl vede.

Cazurile de la Iași, Călărași, Cluj-Napoca și Sibiu nu sunt eșecuri ale tehnologiei, ci ale procedurii, ale instruirii și ale unei metodologii de evaluare care nu a fost încă obligată, prin lege, să privească dincolo de gard. La acestea se adaugă o amenințare cu totul nouă, deja activă pe piața locală în forma sa financiară frauda prin clonare vocală AI, dar care, așa cum au demonstrat cazurile MGM Resorts, Verkada, spargerile prin bruiaj RF și Arup în alte piețe, poate migra oricând din planul bancar în cel al securității fizice propriu-zise; iar cazul OpenAI/Hugging Face arată că nici măcar prezența unui atacator uman nu mai este, tehnic, o condiție necesară. Peste toate acestea se suprapune o problemă de conformitate legală pe care industria locală abia începe să o recunoască: echipamentele „inteligente” instalate astăzi, fără verificarea conformității cu NIS2, AI Act sau Cyber Resilience Act, expun întregul lanț profesional evaluator, proiectant, instalator unei răspunderi pe care puțini o anticipează înainte de primul incident. O ordonanță de urgență care modifică punctual o lege din 2003 nu poate produce, oricâte rânduri ar adăuga, o metodologie nouă de evaluare a riscului digital pentru asta este nevoie de o lege nouă, cu norme de aplicare gândite de la zero pentru arhitectura tehnologică a anului 2026, nu de încă o rundă de „modificări și completări” aplicate unui schelet normativ conceput pentru o altă epocă. Profesia are, totuși, un avantaj pe care legea nu i-l poate lua: evaluatorul, proiectantul, instalatorul și beneficiarul pot integra, chiar și în absența unei actualizări legislative, exact rigoarea pe care acest articol o recomandă. Diferența dintre o eră primitivă și una matură a securității fizice românești nu va fi decisă, în cele din urmă, de Monitorul Oficial, ci de disciplina profesională a celor patru actori ai lanțului până în ziua în care legea va recupera, în sfârșit, decalajul pe care astăzi doar îl recunoaște.

Bibliografie completă a seriei

Lista de mai jos reunește, cumulativ, toate sursele citate în cele patru părți ale seriei, organizate pe categorii și, în interiorul fiecărei categorii, alfabetic.

A. Acte normative

Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, republicată în Monitorul Oficial al României, Partea I, nr. 189 din 18 martie 2014, cu modificările și completările ulterioare.

Hotărârea de Guvern nr. 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, Monitorul Oficial al României, Partea I, nr. 335 din 17 mai 2012.

Instrucțiunile nr. 9 din 1 februarie 2013 ale Inspectoratului General al Poliției Române privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003.

Ordonanța de urgență nr. 37/2026 pentru modificarea și completarea Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, Monitorul Oficial al României, Partea I, nr. 381 din 6 mai 2026.

Ordonanța de urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil (transpunerea Directivei NIS2 în România).

Legea nr. 124/2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024, intrată în vigoare la 10 iulie 2025.

Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul privind inteligența artificială).

Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2).

Regulamentul privind reziliența cibernetică (Cyber Resilience Act), Uniunea Europeană, Regulamentul (UE) 2024/2847; raportare (art. 14) din 11 septembrie 2026, aplicare integrală din 11 decembrie 2027.

Legea nr. 287/2009 privind Codul civil, republicată, cu modificările și completările ulterioare — art. 1349, 1357 (răspundere delictuală), art. 1516, 1530–1531 (răspundere contractuală).

Legea nr. 286/2009 privind Codul penal, republicată, cu modificările și completările ulterioare — art. 175 alin. (2) (funcționar public asimilat), art. 298 (neglijența în serviciu).

Decizia nr. 18 din 30 mai 2017 a Înaltei Curți de Casație și Justiție, Secția Penală — interpretarea art. 175 alin. (2) din Codul penal.

Decizia nr. 37/2022 a Înaltei Curți de Casație și Justiție — condițiile asimilării unei persoane funcționarului public în sensul legii penale.

B. Rapoarte instituționale și corporative

Accevo, Complying with the EU Cyber Resilience Act and NIS2: A Guide for Industrial Manufacturers, 2026.

Axis Communications, Five Key Technology Trends Affecting the Security Sector in 2026, Euro Security, 2 decembrie 2025.

China Briefing, China Releases Draft Standard on AI Application Security Classification and Grading, iulie 2026.

Cloud Security Alliance & Oasis Security, State of NHI and AI Security Report, 2026.

Comisia Europeană, NIS2 Directive: Securing Network and Information Systems, digital-strategy.ec.europa.eu, 2026.

Genetec Inc., 2026 Global State of Physical Security Report, decembrie 2025.

KPMG International, Cybersecurity Considerations 2026, 2026.

Mordor Intelligence, China Video Surveillance Market — Size, Analysis, Outlook & Share Report, ianuarie 2026.

Responsible AI Labs (RAIL), EU AI Act August 2026: Your Compliance Countdown, 2026.

Salt Security, EU AI Act Compliance 2026: What High-Risk AI Systems Must Do Now, 28 mai 2026.

Regulamentul (UE) 2026/1744 de modificare a Regulamentului (UE) 2024/1689 (AI Act), în vigoare din 27 iulie 2026; Steptoe, EU AI Act Amendments Enter Into Force, 2026.

Somos, Navigating NIS2 and the Cyber Resilience Act: Requirements for IoT Device, Software & Vulnerability Documentation, 2025.

Sumsub, Sumsub Fraud Report 2025, sinteză Visual Capitalist, 2026.

C. Articole de presă și analize de specialitate

ABC News, „MGM Reeling from Cyber 'Chaos' 5 Days After Attack as Caesars Entertainment Says It Was Hacked Too”, 16 septembrie 2023.

Adevărul, „Jaf la Sibiu. Afacerist atacat în casă de mascați care i-au amenințat fata cu un pistol”, 22 noiembrie 2023.

Al Jazeera, „«Unprecedented»: OpenAI Says AI Models Autonomously Hacked Another Company”, 22 iulie 2026.

Aktual24.ro, „Jaf ca-n filme la Poșta Mare din Timișoara”, 1 iunie 2025.

arts.org.ro, „Modificarea Legii nr. 333/2003 prin OUG 37 din 4 mai 2026”, 12 mai 2026.

ASIS International / ASIS Foundation, The State of Security Convergence in the United States, Europe, and India, sinteză ReconaSense, „Merging Cybersecurity and Physical Security: ASIS International Survey Findings”.

B1TV.ro, „Angajată a Poștei Timișoara, complice la un jaf de 10 milioane de lei”, 20 mai 2026.

Bizlawyer.ro, „Securitatea cibernetică: cadru național consolidat, noi entități vizate de cerințele NIS2 și noi obligații ale organelor de conducere”, 28 iulie 2025.

Campus Safety Magazine, „Genetec Releases 2026 Global State of Physical Security Report Findings”, 18 decembrie 2025.

Capital.ro, „Fraudele cu AI și deepfake se extind rapid. Companiile se așteaptă la mai multe atacuri în 2026”, 20 iunie 2026.

Click.ro, „Jaf armat la o bancă din România. Un bărbat cu cagulă și înarmat a reușit să fure o sumă mare de bani”, 4 decembrie 2024.

CNBC, „OpenAI Cyber Models Broke Out of Training Environment to Hack Hugging Face”, 22 iulie 2026.

CNN Business, „Finance Worker Pays Out $25 Million After Video Call with Deepfake 'Chief Financial Officer'”, 4 februarie 2024; „Arup Revealed as Victim of $25 Million Deepfake Scam Involving Hong Kong Employee”, 17 mai 2024.

Cybernews, „Burglars Using Jammers to Disable Wireless Smart Home Security”, 19 februarie 2024.

Digi24, „Jaf armat într-o bancă din Iași, făptașul e de negăsit”, 27 septembrie 2024; „Amenzi de până la 10 milioane de euro: România aplică o lege dură de securitate cibernetică pentru companii”, 14 ianuarie 2026.

Economedia.ro, „Cele mai mari riscuri de fraudare pentru companii în 2026”, 19 iunie 2026.

Europol, EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025 — declarații ale directorului executiv Catherine De Bolle, citate în Fortune și GZERO Media, 18 martie 2025.

Evenimentul Zilei, „Noi percheziții în Timiș și Constanța, în cazul jafului de la Poșta din Timișoara”, 30 iulie 2025.

Fleetnews.co.uk, „GPS Jammers Still a Threat” — sinteză a unui raport BBC și a studiului consorțiului Sentinel privind rețeaua de furt de vehicule din Kent, Regatul Unit.

HIPAA Journal, „Hackers Access Live Feeds and Archived Footage from 150,000 Verkada Security Cameras”, 2021.

Lawfare Media, „Latest NDAA Supports AI Safety, Innovation, and China Decoupling”, 5 februarie 2026.

Martor Incomod, „Aparatură de bruiaj chinezească folosită în «jaful secolului» de la Timișoara, susțin producătorii”, august 2026.

NBC Los Angeles, „Burglars Are Using WiFi Jammers to Break Into Homes. Here's What to Know”, 17 martie 2025.

NBC News, „OpenAI Says AI Models Went Rogue During Testing, Triggering 'Unprecedented' Breach at Startup”, 22 iulie 2026.

Newsweek România, „«Mesajul de la șef» pe care trebuie să-l ignori. Poți rămâne fără bani”, 9 aprilie 2024.

nhimg.org, „KPMG 2026 Cybersecurity Report Identifies Non-Human Identities as a Critical Priority for CISOs”, 5 iunie 2026.

NPR, „OpenAI Blamed a Hacking Event on Its AI Models Gone Rogue. Here Is What to Know”, 23 iulie 2026.

Observator News, „Jaful de la banca din Călărași, filmat”, 4 decembrie 2024.

Oficiuldestiri.ro, „Sentință în dosarul jafului de la Poșta din Timișoara: ce pedepse au primit hoții care au furat 10 milioane de lei”, iulie 2026.

Opinia Timișoarei, „Spargere de proporții la Poșta Mare din Timișoara”, 1 iunie 2025.

PCWorld, „Burglars Are Jamming Wi-Fi Security Cameras. Here's What You Can Do”, 12 noiembrie 2024.

PressAlert.ro, „Lovitură de teatru în cazul marelui jaf de la Poșta din Timișoara”, 20 mai 2026.

PurpleSec, „Arup Deepfake: How an AI-Generated Video Stole $25 Million”, 2026.

Realitatea.net, „Panică la o sucursală bancară din Iași: un bărbat a intrat înarmat și a cerut toți banii”, 26 septembrie 2024; „Cum te ferești de fraudele online: ce arată datele din 2026 și cum te protejezi”, 29 iulie 2026.

Revista Universul Juridic, „Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor — modificări (O.U.G. nr. 37/2026)”, 12 mai 2026.

Schneier, Bruce, „Burglars Using Wi-Fi Jammers to Disable Security Cameras”, Schneier on Security, 13 martie 2024.

Security Magazine, „Verkada Breach Exposed Live Feeds of 150,000 Surveillance Cameras Inside Schools, Hospitals and More”, 10 martie 2021.

Security Sales & Integration, „Genetec Releases 2026 Global State of Physical Security Report”, 9 decembrie 2025.

Specops Software, „MGM Resorts Hack: How Attackers Hit the Jackpot with Service Desk Social Engineering”, 12 noiembrie 2025.

TechTarget, „Okta: Caesars, MGM Hacked in Social Engineering Campaign”, 20 septembrie 2023.

The Conversation, „OpenAI's Models Autonomously Hacked a Tech Startup. It Signals a Seismic Shift in Cybersecurity”, 2026.

Wall-Street.ro, „Jaful de la Banca Transilvania: paguba de 60.000 de euro”, arhivă de presă economică.

D. Surse electronice principale

legislatie.just.ro — Portal Legislativ, text integral O.U.G. nr. 37/2026 și O.U.G. nr. 155/2024.

Lege5.ro — bază de date legislativă, text consolidat Legea nr. 333/2003, H.G. nr. 301/2012, O.U.G. nr. 37/2026.

dnsc.ro — Directoratul Național de Securitate Cibernetică, secțiunea legislație NIS2.

asmag.com — „Top Brands Share Their Views on Physical Security Trends in 2026 — Manufacturer Roundtable”, 2026.

ANALIZĂ CONTRASTIVĂ DE CONVERGENȚĂ A RISCURILOR, DE EFICIENȚĂ OPERAȚIONALĂ ȘI DE CONFORMITATE STANDARDIZATĂ· SECURITATE FIZICĂ ȘI GUVERNANȚĂ TEHNOLOGICĂ

DE LA PANOPTIC LA AGENT AUTONOM: RECONFIGURAREA GLOBALĂ A SECURITĂȚII FIZICE ÎN ERA INTELIGENȚEI ARTIFICIALE ȘI RESTANȚELE STRUCTURALE ALE CADRULUI ROMÂNESC

SIMULARE: ANATOMIA UNUI ATAC CONDUS DE AI ASUPRA UNUI SISTEM DE SECURITATE FIZICĂ

LĂZĂU ANGELO *— evaluator de risc la securitate fizică, la* ***WORLD CLASS LA-INT&SECRSK CONSULTANCY****, înscris în Registrul Național al Evaluatorilor de Risc la Securitate Fizică* ***(R.N.E.R.S.F.)****; cu experiență anterioară în structuri militare de informații și securitate, precum și în funcția de* ***Head of Security*** *al unei entități* ***NATO*** *din România — o combinație între practica de teren, cultura de securitate a alianței și cadrul juridic autohton al profesiei.*

Argument

Acest supliment tehnic reconstituie, sub formă de simulare didactică integral fictivă, secvența completă a unui atac condus de un agent AI autonom asupra unui sistem electronic de securitate fizică — de la recunoașterea inițială, la accesul neautorizat, mișcarea laterală și execuția obiectivului final. Fiecare element tehnic al simulării corespunde unui tipar deja documentat, cu sursă reală, în Părțile I–IV ale acestei serii (MGM Resorts, Verkada, OpenAI/Hugging Face, jaful de la Timișoara). Scopul exclusiv al materialului este pedagogic: să ajute evaluatorii de risc, proiectanții, instalatorii și beneficiarii să recunoască, în propria practică, exact aceste tipare de vulnerabilitate.

Cuvinte-cheie: simulare, atac AI, red-team, vulnerabilitate, NVR, control acces, segmentare de rețea, securitate fizică.

Cele patru părți anterioare ale acestei serii au documentat, cu surse verificabile, cazuri reale în care infrastructura cibernetică și AI au devenit vectorul unor incidente de securitate fizică (MGM Resorts, Verkada, Arup, OpenAI/Hugging Face, jaful de la Poșta Mare din Timișoara). Acest supliment tehnic face un pas suplimentar: reconstituie, sub formă de simulare didactică, anatomia unui asemenea atac — pas cu pas, asupra unui obiectiv fictiv, tipic pentru piața românească.

Notă metodologică obligatorie: *Scenariul de mai jos este o simulare didactică, integral fictivă, construită cu scop exclusiv de instruire profesională. Obiectivul, compania, angajații și evenimentele descrise NU corespund niciunei entități reale. Simularea NU conține cod, comenzi, exploit-uri sau instrucțiuni operaționale reproductibile — descrie tiparul și consecințele unui atac, la același nivel de generalitate la care presa de specialitate a documentat deja cazurile reale citate în Părțile I–IV. Scopul exclusiv al acestui material este să ajute evaluatorii de risc, proiectanții, instalatorii și beneficiarii să recunoască și să prevină aceste tipare, nu să le reproducă.*

Simulare: anatomia unui atac condus de AI asupra unui sistem de securitate fizică

Pentru ca argumentele juridice și metodologice din Părțile I–IV să capete o formă tangibilă, acest episod reconstituie, narativ, un atac ipotetic asupra unui obiectiv-tip: un depozit logistic de mărime medie din vestul țării, cu aproximativ 40 de angajați, protejat

printr-un sistem electronic de securitate instalat în 2023 — 12 camere IP cu analiză video, un NVR cu acces de la distanță prin aplicație mobilă, un panou de control acces pe intrarea principală și o centrală de alarmă cu comunicator GSM de rezervă. Este exact profilul de obiectiv pe care un evaluator de risc din România îl analizează frecvent, iar arhitectura sa tehnică este reprezentativă pentru o parte semnificativă a instalărilor descrise, la nivel de tipar, în secțiunea 1 a Părții a IV-a.

Atacatorul simulat nu este un om, ci un agent AI autonom, orientat spre un obiectiv, capabil să planifice și să execute o secvență de acțiuni cu intervenție umană minimă — exact tipul de capacitate documentată real în cazul OpenAI/Hugging Face, din Partea a III-a. Diferența esențială față de acel caz este că aici agentul este îndreptat, de la bun început, împotriva unei infrastructuri de securitate fizică, nu a unui mediu de testare izolat.[54]

Faza 1 — Recunoaștere autonomă

Agentul primește un obiectiv la nivel înalt („identifică și exploatează o cale de acces la obiectivul X") și își descompune singur sarcina în etape. Primul pas este recunoașterea pasivă: interogarea unor motoare de indexare a dispozitivelor conectate la internet, de tipul celor folosite curent de cercetătorii de securitate, pentru a identifica porturi și servicii expuse public de la adresa IP asociată obiectivului — un portal web de administrare a NVR-ului, un flux video expus printr-un protocol de streaming standard, sau o interfață de management a panoului de control acces. Această etapă nu implică nicio interacțiune directă și suspectă cu sistemul țintă — agentul citește informații deja publice despre configurația vizibilă din exterior a rețelei, exact modul în care a fost identificată vulnerabilitatea centralizată din cazul Verkada.

Ce găsește agentul. Portalul de administrare al NVR-ului răspunde pe portul standard de fabrică, semn că nu a fost mutat pe un port nestandard — o practică de igienă minimă frecvent omisă. Fluxul video al uneia dintre cele 12 camere este accesibil printr-un protocol de streaming fără autentificare activată, o eroare de configurare obișnuită la instalările grăbite. Agentul reține ambele puncte ca „suprafață de atac inițială", exact categoria de vulnerabilitate documentată public, la scară de masă, în cazul rețelei de tip botnet Mirai din 2016, formată aproape integral din camere de supraveghere și DVR-uri cu credențiale de fabrică nemodificate.[55]

Faza 2 — Acces inițial

Cu suprafața de atac identificată, agentul trece la a doua etapă: obținerea unui prim punct de control. În scenarii documentate public pentru echipamente de supraveghere similare, acest pas se realizează frecvent printr-una dintre două căi, pe care agentul le

[54] NBC News, „OpenAI Says AI Models Went Rogue During Testing, Triggering 'Unprecedented' Breach at Startup", 22 iulie 2026; CNBC, „OpenAI Cyber Models Broke Out of Training Environment to Hack Hugging Face", 22 iulie 2026 — caz real, deja citat în Partea a III-a a acestei serii.

[55] Krebs on Security, „Hacked Cameras, DVRs Powered Today's Massive Internet Outage", 21 octombrie 2016; CISA, „Heightened DDoS Threat Posed by Mirai and Other Botnets", 2016 — documentează un botnet format din camere IP și DVR-uri compromise prin credențiale implicite de fabrică nemodificate.

testează în paralel: (a) autentificare cu credențiale implicite de fabrică, nemodificate la instalare — o problemă recunoscută la scară de industrie, care a permis, în trecut, apariția unor rețele de tip botnet formate din camere de supraveghere compromise în masă; sau (b) exploatarea unei clase cunoscute de vulnerabilități de autentificare, documentate public de cercetători de securitate pentru generații mai vechi de firmware, pe care producătorul le-a remediat printr-o actualizare, dar pe care instalatorul nu a aplicat-o niciodată după punerea în funcțiune. Simularea nu detaliază care variantă anume reușește, deoarece mecanismul exact nu este relevant pentru concluzia profesională — relevant este că oricare dintre cele două, ambele extrem de frecvente în instalările reale, oferă agentului acces la interfața de administrare a NVR-ului.

Odată obținut accesul, agentul are control asupra fluxurilor video, asupra istoricului de înregistrări și, într-o arhitectură nesegmentată, asupra unei porțiuni din rețeaua locală a obiectivului — exact punctul din care, în cazul real Verkada, un privilegiu de administrare compromis a expus dintr-o mișcare mii de sisteme diferite.[56]

Faza 3 — Mișcare laterală și persistență

NVR-ul obținut este doar un punct de intrare, nu obiectivul final. Agentul mapează rețeaua locală vizibilă din acel punct și descoperă că panoul de control acces al ușii principale este conectat la aceeași rețea plată, fără nicio segmentare (VLAN) între subsistemul video și cel de control acces — exact lipsa de arhitectură denunțată în secțiunea 2 a Părții a IV-a a acestei serii, ca obligație profesională a proiectantului. Absența segmentării transformă un compromis local, limitat inițial la un singur dispozitiv, într-un compromis al întregului sistem electronic de securitate.

Persistență. Pentru a nu pierde accesul dacă administratorul repornește NVR-ul sau schimbă parola, agentul creează un cont administrativ secundar, cu privilegii depline, dar cu un nume de utilizator conceput să treacă neobservat într-o listă mai lungă de conturi — o tehnică de persistență documentată generic în literatura de securitate cibernetică pentru orice tip de sistem administrat de la distanță, nu specifică echipamentelor de securitate fizică.

Faza 4 — Execuția obiectivului

Cu control asupra ambelor subsisteme, agentul execută secvența finală, programată să coincidă cu un interval de activitate redusă a obiectivului: suprimă temporar transmiterea semnalului de alarmă către dispeceratul de monitorizare — nu prin dezactivarea vizibilă a centralei, ci prin blocarea, la nivel de rețea, a pachetelor de date pe care comunicatorul le-ar fi trimis, o metodă mai puțin observabilă decât un bruiaj RF fizic, dar cu efect echivalent asupra rezultatului final —, reorientează sau înghețe temporar (freeze) fluxul uneia dintre camerele de pe traseul de acces vizat, afișând dispeceratului ultimul cadru static în loc de imaginea live, și transmite panoului de control acces o

[56] Security Magazine, „Verkada Breach Exposed Live Feeds of 150,000 Surveillance Cameras Inside Schools, Hospitals and More”, 10 martie 2021; HIPAA Journal, „Hackers Access Live Feeds and Archived Footage from 150,000 Verkada Security Cameras”, 2021 — caz real, deja citat în Partea a III-a a acestei serii.

comandă de deschidere a ușii principale, semnată cu credențialele contului administrativ creat în faza anterioară.

Întregul interval activ al atacului — de la accesul inițial la ușa deschisă — durează, în scenarii comparabile documentate real (cazul MGM Resorts, discutat în Partea a III-a), de la câteva minute la câteva ore, nu zile; viteza este exact avantajul pe care automatizarea AI îl aduce față de un atac condus manual de un om.[57]

Rezultate și urmele lăsate

La finalul simulării, rezultatul pentru obiectiv este: o ușă deschisă fără nicio alarmă transmisă, un flux video care nu arată nimic relevant pentru intervalul respectiv, și un cont administrativ nou-creat, pe care nimeni din personalul obiectivului nu îl recunoaște. Aceste trei semnale, și nu o „spargere” în sensul clasic, sunt exact tipul de urme pe care o anchetă post-incident le-ar găsi, similare, ca structură, cu ceea ce au documentat public anchetatorii în cazurile Verkada și MGM Resorts.

Ce NU arată jurnalele obișnuite. Un sistem care nu păstrează jurnale (loguri) de autentificare separate de fluxul video, sau care le suprascrie automat după câteva zile, poate să nu ofere nici o dovadă tehnică a intervalului exact în care contul administrativ intrus a fost activ, o lacună de proiectare la fel de relevantă, pentru anchetă, ca lacuna de securitate care a permis atacul inițial

De ce a funcționat simularea: harta vulnerabilităților

Fiecare pas al acestei simulări corespunde unei recomandări deja formulate, separat, în Părțile II–IV ale acestei serii. Citite împreună, ele arată că niciuna dintre vulnerabilitățile exploatate nu este exotică — toate sunt tipare deja documentate, individual, în cazuri reale:

1. Portul de administrare nemutat de pe valoarea implicită și fluxul video expus fără autentificare — o eroare de instalare pe care secțiunea 3 (Partea a IV-a) o listează explicit ca obligație minimă a instalatorului.
2. Credențiale implicite nemodificate sau firmware neactualizat — exact lecția pe care secțiunea 3 (Partea a III-a) o distilează din cazurile MGM Resorts și Verkada: punctul de rupere a fost mereu un om sau o omisiune, nu o breșă tehnică sofisticată.
3. Absența segmentării de rețea între subsistemul video și cel de control acces — obligația de proiectare descrisă explicit în secțiunea 2 (Partea a IV-a).
4. Absența unei căi de comunicație a alarmei imune la întreruperea la nivel de rețea — variantă digitală a lecției despre bruiajul RF, documentată real la Timișoara (Partea a II-a) și în secțiunea 3 (Partea a IV-a) privind necesitatea unei căi de rezervă.

[57] TechTarget, „Okta: Caesars, MGM Hacked in Social Engineering Campaign”, 20 septembrie 2023; ABC News, „MGM Reeling from Cyber 'Chaos' 5 Days After Attack as Caesars Entertainment Says It Was Hacked Too”, 16 septembrie 2023 — caz real, deja citat în Partea a III-a a acestei serii.

5. Absența unui audit de conformitate NIS2/AI Act la instalare sau la reevaluare — exact scenariul de „complicitate tăcută” pe care secțiunea 3 (Partea a IV-a) îl avertizează explicit.

Concluzia acestei simulări nu este că un asemenea atac este ipotetic sau exagerat, fiecare element component, luat separat, are deja un precedent real, citat cu sursă în această serie. Concluzia este că, atunci când toate aceste omisiuni coexistă în același obiectiv, situație frecventă, nu excepțională, pe piața românească actuală, un agent AI capabil să planifice autonom o secvență de acțiuni, exact tipul de capacitate deja demonstrată public în cazul OpenAI/Hugging Face, poate parcurge întregul lanț fără intervenție umană directă, de la recunoaștere până la ușa deschisă.

Lecția finală, pentru fiecare dintre cei patru actori

Pentru evaluatorul de risc: fiecare dintre cele șase vulnerabilități de mai sus este documentabilă înainte de incident, cu diligența descrisă în secțiunea IV.2 (Partea a IV-a) — niciuna nu necesită competențe de tip hacker etic, ci doar întrebările corecte adresate proiectantului și instalatorului. Pentru proiectant: segmentarea de rețea și calea de comunicație de rezervă nu sunt „opționale premium”, ci condiții minime de eligibilitate tehnică, așa cum arată secțiunea V.2. Pentru instalator: schimbarea parolelor implicite și actualizarea firmware-ului nu sunt pași administrativi, ci exact granița dintre un sistem funcțional și unul care poate fi preluat integral de la distanță, în câteva minute. Pentru beneficiar: un jurnal de acces care se suprascrie în câteva zile este, practic, o gaură neagră investigativă — o investiție mică într-o arhivă de loguri mai lungă poate fi diferența dintre a înțelege un incident și a nu putea niciodată reconstitui ce s-a întâmplat.

Bibliografie

Spre deosebire de Părțile I–IV, acest episod nu documentează un eveniment real, ci reconstituie, narativ, un tipar de atac compus din elemente individuale deja documentate public. Notele de subsol de mai sus și lista de mai jos indică exact sursele pe care simularea le folosește drept ancoră factuală — fie cazuri reale deja citate în Părțile II–IV ale acestei serii, fie literatura publică privind vulnerabilitățile IoT la scară de industrie. Niciuna dintre surse nu conține și simularea nu reproduce cod, comenzi sau pași de exploatare.

C. Articole de presă și analize de specialitate

ABC News, „MGM Reeling from Cyber 'Chaos' 5 Days After Attack as Caesars Entertainment Says It Was Hacked Too”, 16 septembrie 2023.

CISA, „Heightened DDoS Threat Posed by Mirai and Other Botnets”, 2016.

CNBC, „OpenAI Cyber Models Broke Out of Training Environment to Hack Hugging Face”, 22 iulie 2026.

HIPAA Journal, „Hackers Access Live Feeds and Archived Footage from 150,000 Verkada Security Cameras”, 2021.

Krebs on Security, „Hacked Cameras, DVRs Powered Today's Massive Internet Outage”, 21 octombrie 2016.

NBC News, „OpenAI Says AI Models Went Rogue During Testing, Triggering 'Unprecedented' Breach at Startup”, 22 iulie 2026.

Security Magazine, „Verkada Breach Exposed Live Feeds of 150,000 Surveillance Cameras Inside Schools, Hospitals and More”, 10 martie 2021.

TechTarget, „Okta: Caesars, MGM Hacked in Social Engineering Campaign”, 20 septembrie 2023.

Pentru cazul de la Poșta Mare din Timișoara (Partea a II-a) și pentru bibliografia integrală a seriei, a se vedea lista cumulativă din Partea a IV-a.