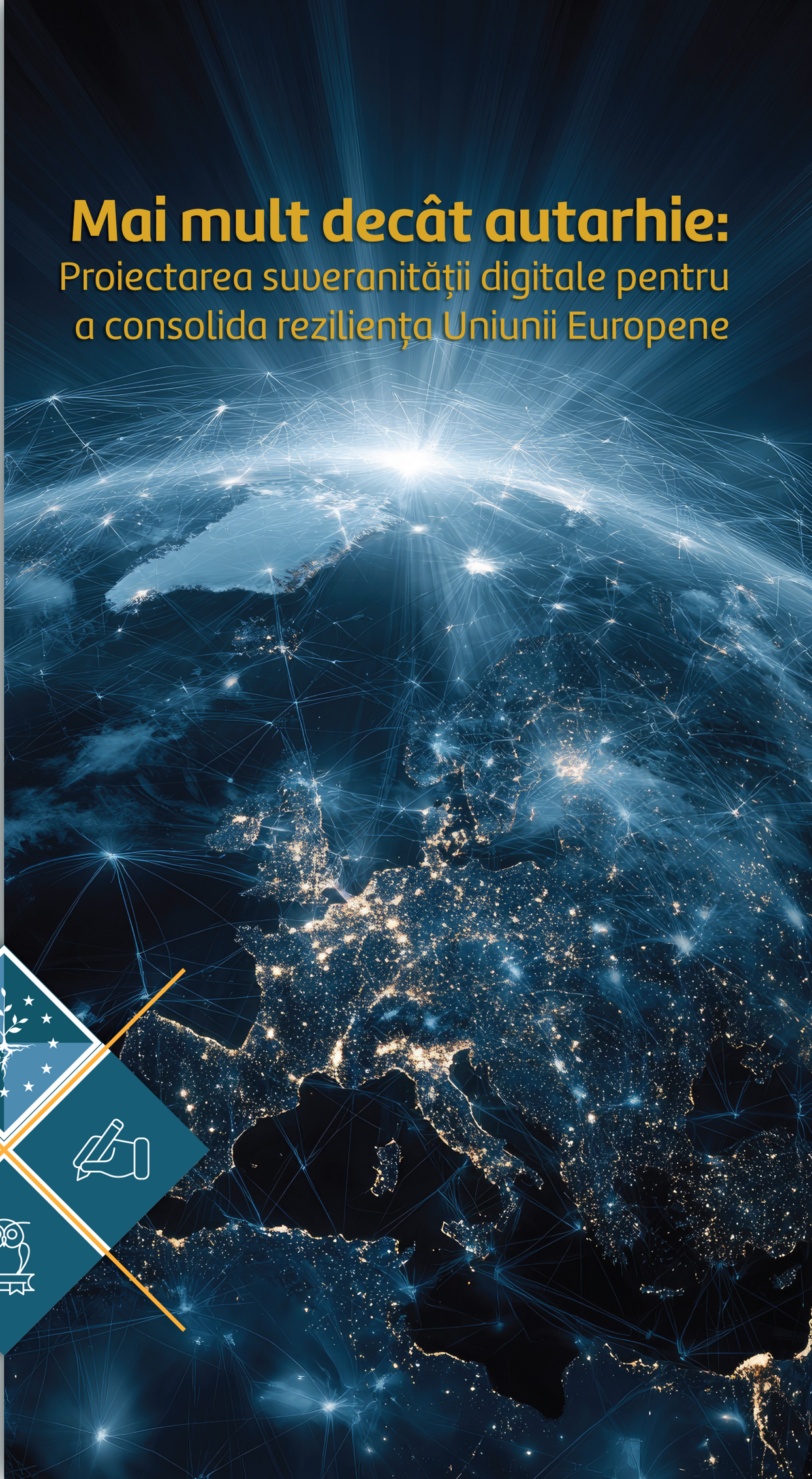
RESILIENCE ESSAYS

Mai mult decât autarhie:

Proiectarea suveranității digitale pentru a consolida reziliența Uniunii Europene



CENTRUL EURO-ATLANTIC
PENTRU REZILIENȚĂ

EURO-ATLANTIC
RESILIENCE CENTRE

Centrul Euro-Atlantic pentru Reziliență (E-ARC) este o structură de expertiză în domeniul rezilienței menită sa ofere instrumente de lucru statelor UE și NATO. Centrul funcționează ca o platformă de comunicare între autoritățile publice, spațiul academic, societatea civilă, mediul de afaceri și orice altă voce relevantă în domeniu. Centrul are propriile proiecte de cercetare, dar oferă și programe de pregătire pentru viitorii experți în domeniul rezilienței.

Misiunea E-ARC este aceea de a scana un orizont cât mai vast, încercând să anticipeze următoarea criză majoră, să pregătească societatea pentru neașteptat și să identifice de timpuriu semnalele de alertă. Rezultatele cercetărilor E-ARC sunt transpuse în ghiduri destinate autorităților, dar Centrul se adresează în egală măsură publicului larg, pentru a consolida reziliența pe toate palierele societății.

Publicat de Centrul Euro-Atlantic pentru Reziliență
Str. Vasile Lascăr nr. 52, Sector 2, București
www.e-arc.ro | contact@e-arc.ro | +40 21 369 54 30

Mai mult decât autarhie:
Proiectarea suveranității digitale pentru a consolida reziliența Uniunii Europene

de Paul Mândraș

01 Introducere

Atacul de tip ransomware din februarie 2024, care a perturbat operațiunile a douăzeci și șase de spitale din România, ilustrează un tipar recurent în peisajul amenințărilor cibernetice din Europa (DNSC, 2024). Atacul informatic asupra unui singur furnizor, care asigura un sistem informatic spitalicesc utilizat pe scară largă, a fost suficient pentru a se răspândi în cascadă în mai multe instituții medicale românești, afectând furnizarea asistenței medicale și punând presiune asupra serviciilor de urgență. Incidentul nu a necesitat exploatări avansate de tip „zero-day" sau capacități cibernetice ofensive sofisticate ale unui actor statal. În schimb, s-a bazat pe vulnerabilități bine-cunoscute, vectori de acces comuni și un ecosistem de dependență digitală.

Acesta este paradoxul din centrul dezbaterii privind suveranitatea digitală și motivul pentru care este importantă pentru securitatea cibernetică. Urmărirea de către UE a suveranității sale digitale declanșează adesea acuzații de protecționism sau naționalism tehnologic (Marco și colab., 2025). Criticii avertizează că urmărirea unui control suveran deplin asupra cloud-urilor, cipurilor și fluxurilor de date va fragmenta spațiul cibernetic, va împiedica cooperarea transfrontalieră și, în cele din urmă, va slăbi apărarea europeană. În contrapartidă, susținătorii suveranității european evidențiază faptul că, fără o autoritate semnificativă asupra infrastructurii sale digitale, Europa rămâne strategic vulnerabilă la coerciție, spionaj și perturbări sistemice din partea unor actori ale căror interese diferă de ale sale.

Ambele poziții conțin unele elemente de adevăr. În același timp, incidentele cibernetice din UE continuă să crească în amploare și sofisticare (Consiliul European, 2025), vizând din ce în ce mai mult nu doar rețelele și datele, ci și încrederea, procesul decizional și coeziunea societăților democratice europene. În acest nou mediu, securitatea cibernetică nu mai poate fi tratată doar ca o problemă pur tehnică. Este o chestiune strategică de putere, dependență și reziliență.

Acest eseu argumentează ideea că suveranitatea digitală poate promova interesele de securitate ale Europei, dar numai dacă este concepută drept un format strategic, centrat pe om și orientat înspre reziliență, mai degrabă decât o

acțiune defensivă de izolare tehnologică. UE trebuie să abordeze suveranitatea digitală ca o strategie de reziliență: una care gestionează dependența, păstrează integritatea democratică și consolidează capacitatea societăților, guvernelor și a instituțiilor de a absorbi și de a se adapta la șocurile digitale.

Provocarea centrală nu este dacă Europa ar trebui să fie suverană în domeniul digital, ci cum poate fi exercitată suveranitatea fără a submina însăși interdependența pe care o necesită securitatea cibernetică modernă.

02 Suveranitatea ca dilemă de securitate

Dilema clasică a securității evidențiază faptul că măsurile defensive ale unui stat pot părea amenințătoare pentru celelalte state, declanșând o stare de insecuritate reciprocă, care se manifestă chiar și în absența unei intenții ostile (Tang, 2009). În era digitală, această dilemă se extinde dincolo de teritoriul fizic, la infrastructură, date și capacitate tehnologică.

Atunci când statele urmăresc să își asigure suveranitatea digitală — prin localizarea datelor, controlul lanțului de aprovizionare sau capacități cibernetice — o fac din motive defensive legitime. Totuși, aceleași măsuri generează suspiciune. Dezvoltarea de capabilități cibernetice dezvoltate pentru protecție digitală poate fi percepută drept o pregătire pentru ofensă. Ambiguitatea dintre apărare și atac în spațiul cibernetic alimentează neîncrederea și insecuritatea.

Această dilemă este agravată de natura spațiului cibernetic în sine. Spre deosebire de granițele teritoriale, care sunt fizice și palpabile, „granițele" digitale sunt conceptuale, poroase și contestate. Amenințările cibernetice traversează jurisdicțiile instantaneu. Astfel, trei dinamici intensifică această dilemă. În primul rând, acțiunile defensive invită la suspiciuni: capacitățile de supraveghere și contrainformații destinate protecției par a fi imposibil de distins de instrumentele ofensive. În al doilea rând, asimetriile de putere cibernetică adâncesc instabilitatea: suveranitatea digitală nu este disponibilă în mod egal tuturor statelor, iar concentrarea controlului tehnologic la nivelul câtorva actori creează vulnerabilități structurale. În al treilea rând, modelele de guvernare

concurente se „ciocnesc" și în spațiul cyber: abordările liberal-democratice care pun accentul pe drepturi și deschidere intră în conflict cu modelele autoritare care prioritizează controlul, fiecare considerându-l pe celălalt un vector de subversiune.

Pentru Uniunea Europeană, dilema ia o formă particulară. În prezent, Europa nu are autonomia necesară pentru a exercita pe deplin această putere cibernetică. Dependența UE de furnizori externi pentru straturile critice ale ecosistemului digital - de la infrastructura cloud și rețelele 5G până la semiconductorii care le alimentează - creează o dinamică de „întrerupător ucigaș" (Rudolph, 2025). Atunci când serviciile esențiale sunt guvernate de actori statali străini sau de „monarhii digitale" globale (Boehler, 2024) , disponibilitatea operațională a Europei este practic ținută ostatică deciziilor luate în Silicon Valley sau Shenzhen. Astfel, acțiunea europeană colectivă este necesară pentru a contracara presiunile externe din partea principalilor jucători din domeniul tehnologiei, însă statele membre rămân reticente în a ceda controlul asupra securității naționale. Această fragmentare creează lacune jurisdicționale și vulnerabilități naționale pe care adversarii le exploatează fără scrupule (Madiega, 2020).

Dilema securității în materie de suveranitate digitală nu poate fi eliminată, dar efectele sale pot fi atenuate prin transparență, mecanisme de răspuns coordonate la nivel european și angajament național.

03 Capcana izolaționismului: când suveranitatea slăbește apărarea

Deținerea suveranității implică, de asemenea, costuri și riscuri. Dacă este conceptualizată drept o autosuficiență tehnologică deplină, suveranitatea digitală poate slăbi securitatea, în loc să o consolideze. Amenințările cibernetice sunt în mod inerent transnaționale, iar apărarea eficientă depinde de schimbul rapid de informații. Localizarea excesivă a datelor sau standardele naționale divergente riscă să fragmenteze spațiul digital al Europei, atât la nivelul individual al statelor membre, cât și la nivelul UE în sine, creând puncte oarbe prin izolarea cercetării europene de inovația globală, mai ales în domenii precum inteligența artificială și tehnologiile cuantice.

O abordare rigidă sau protecționistă poate declanșa, de asemenea, o dilemă de

securitate cibernetică și politică. Măsurile defensive, inclusiv restricțiile lanțului de aprovizionare, pot fi percepute de parteneri ca fiind coerciții economice, subminând încrederea în cadrul alianțelor precum NATO și slăbind apărarea colectivă.

Prin urmare, suveranitatea digitală trebuie concepută pentru a susține interdependența, nu izolarea, iar valoarea sa constă în trei funcții. În primul rând, oferă vizibilitate strategică prin cartografierea dependențelor tehnologice și identificarea punctelor de vulnerabilitate. În al doilea rând, restabilește responsabilitatea politică, impunând responsabilitatea pentru securitatea digitală drept o ancoră a autorității publice, mai degrabă decât dispersând răspunderea între mai mulți actori privați sau străini. În al treilea rând, ajută la protejarea domeniului cognitiv împotriva dezinformării și manipulării, protejând procesele democratice fără a adopta controale autoritare.

Însă, suveranitatea în sine este insuficientă. Fără coordonare, aceasta poate fragmenta ecosistemul digital al Europei și poate reduce reziliența la nivel național și european. O securitate cibernetică eficientă necesită deschidere, încredere, informații partajate și sisteme interoperabile. Supra-securizarea riscă să erodeze fundamentele normative ale Europei și chiar și drepturile fundamentale ale cetățenilor europeni. Obiectivul suveranității moderne nu poate fi controlul total, ci selectivitatea strategică: autarhie acolo unde este necesar, interdependență acolo unde este posibil și cooperare acolo unde este esențial.

04 Proiectarea rezilienței: o abordare cu trei piloni

Pe cale de consecință, cum ar trebui concepută suveranitatea digitală pentru a consolida reziliența europeană? Aceasta necesită o îmbunătățire conceptuală: de la o perspectivă asupra securității centrată pe hardware și software, la un model holistic care integrează reglementarea, societatea și inovația. În plus, suveranitatea digitală trebuie înțeleasă drept un instrument pentru reziliență – capacitatea de a avansa prin absorbția șocurilor, adaptare și menținerea funcțiilor de bază. Aceasta necesită o permutare de la izolaționism la holism, iar o abordarea noastră bazată pe trei piloni surprinde exact această logică.

Pilonul 1: Selectivitate strategică prin autonomia reglementării

Puterea Europei nu constă în autosuficiența totală, ci în puterea de reglementare. Prin instrumente precum GDPR, NIS2 ori Legea UE privind inteligența artificială, UE exportă standarde de securitate la nivel global. Acest „Efect Bruxelles" sporește reziliența prin forțarea tehnologiilor străine să funcționeze în termeni europeni, cu respectarea valorilor noastre societale: transparență, interoperabilitate și securitate (Bradford, 2020). Astfel, suveranitatea europeană se exercită prin reguli, nu prin ziduri.

Pilonul 2: Reziliență inovativă prin agilitatea public-privată

Securitatea cibernetică nu se poate baza pe apărări statice. Reziliența depinde de viteză, adaptabilitate și inovație, iar parteneriatele public-private solide sunt esențiale pentru a partaja informații despre amenințări în timp real și pentru a răspunde mai rapid decât adversarii. Statul trebuie să mențină controlul tehnologic strategic, valorificând în același timp agilitatea sectorului privat, dar investind selectiv în tehnologii critice, evitând dependențe catastrofale (Mândraș, 2024).

Pilonul 3: Dimensiunea umană printr-un firewall cognitiv și emoțional

Amenințările moderne țintesc societățile și oamenii la fel de mult ca sistemele tehnice. Dezinformarea, deepfake-urile și manipularea algoritmică exploatează vulnerabilitățile cognitive și emoționale individuale, iar tocmai din această cauză, suveranitatea digitală trebuie să includă și cetățenii. Prin urmare, educația pentru gândire critică, transparența în guvernanța algoritmică și protejarea încrederii societale sunt esențiale. O infrastructură digitală suverană este lipsită de sens fără un public rezilient la dezinformare și capabil să reziste manipulării ostile.

Prin urmare, suveranitatea digitală trebuie să se extindă dincolo de tehnologie pentru a include o abordare centrată pe om, care să consolideze reziliența societală împotriva amenințărilor cognitive și informaționale. Împreună, aceste măsuri vizează protejarea valorilor democratice și prevenirea dezmembrării politicilor de securitate în autoritarism ori dictatură digitală. Pe scurt, suveranitatea orientată înspre reziliență nu înseamnă izolare sau control total, ci proiectarea unei guvernanțe, a unor piețe și a unor societăți care pot rezista presiunii fără a abandona deschiderea, cooperarea sau valorile democratice

Concluzie: Suveranitatea ca influență și autonomie fără izolare

04

Suveranitatea digitală susține interesele Europei în materie de securitate cibernetică, dar numai dacă este înțeleasă ca formă de putere cibernetică prin acțiuni și influență, nu prin izolare și inacțiune. Într-un mediu digital interconectat și contestat permanent, dependența creează vulnerabilitate, însă retragerea în autarhia tehnologică ar slăbi reziliența în mod determinant, în loc să o consolideze.

Dacă este concepută corespunzător, suveranitatea digitală este echivalentă cu o arhitectură de reziliență: folosește reglementarea pentru a modela tehnologiile globale, investițiile strategice pentru a reduce dependențele critice și educația pentru a proteja domeniul uman și cognitiv. Scopul suveranității în spațiul digital nu este de a izola Europa și statele sale membre, ci de a permite o implicare în termeni europeni: deschisă acolo unde este posibil, autonomă acolo unde este necesar.

În cele din urmă, adevărata măsură a succesului european nu va consta în absența incidentelor cibernetice, ci va proveni din capacitatea de a le contracara, fără a pierde în cele din urmă încrederea, coeziunea sau integritatea democratică. Într-o eră a concurenței digitale permanente, suveranitatea nu se poate obține prin construirea de „ziduri" mai înalte, ci prin dezvoltarea de acțiuni care să ne asigure că, atunci când „cetatea" digitală este atacată - așa cum se va întâmpla inevitabil - societățile europene rămân coerente, adaptive, coezive și libere.

Aceasta este reziliența. Și tocmai de aceea suveranitatea digitală, concepută corespunzător, nu reprezintă o renunțare la interdependență, ci o condiție pentru menținerea acesteia.

06 Referințe

Boehler, P. (2024, noiembrie 27). From digital monarchies to decentralized republics: Social media protocols are political. https://www.pboehler.net/fediverse-nostr-protocol/

Bradford, A. (2020). Brussels effect. How the European Union Rules the World (Oxford University Press). https://www.brusselseffect.com/

DNSC. (2024, februarie 15). ALERTĂ: Backmydata Ransomware. Directoratul National de Securitate Cibernetică. https://www.dnsc.ro/citeste/alert-backmydata-ransomware-spitale-romania

European Council. (2025, iunie 30). Cyber threats in the EU: facts and figures. European Council. https://www.consilium.europa.eu/en/policies/top-cyber-threats/#0

Madiega, T. (2020). Digital sovereignty for Europe. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI%282020%29651992_EN.pdf

Mândraș, P. (2024). Innovative Resilience for Civil Defence Human-Digital Ecosystems. A Theoretical Framework. Euro-Atlantic Resilience Journal, 2(4), 59-92. https://resiliencejournal.e-arc.ro/wp-content/uploads/2024/12/EARJ-4-2024-Mandras-Innovative-Resilience.pdf

Marco, D. D., Gonzalez, S. T., Kotsev, A., Friis-Christensen, A., King, M., & Minghini, M. (2025). Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty. https://publications.jrc.ec.europa.eu/repository/handle/JRC144908

Rudolph, T. H. (2025, august 28). A 'Kill Switch' Could Shutter Europe's Access to US Tech. Here's How. TechPolicy. Press. https://www.techpolicy.press/washington-could-activate-a-kill-switch-to-terminate-european-access-to-us-tech-heres-how-it-could-work/

Tang, S. (2009). The Security Dilemma: A Conceptual Analysis. Security Studies, 18(3), 587-623. https://doi.org/10.1080/09636410903133050

Publicat de Centrul Euro-Atlantic pentru Reziliență
Strada Vasile Lascăr nr. 52, Sector 2, București
www.e-arc.ro | contact@e-arc.ro | +40 21 369 54 30

Pentru a consulta și alte studii ale experților E-ARC, vă invităm să scanați codul QR alăturat:

Centrul Euro-Atlantic pentru Reziliență
Martie 2026