STRATEGII DE APĂRARE CIBERNETICĂ ÎN SECTORUL SĂNĂTĂȚII: DESCURAJARE, REZILIENȚĂ ȘI PROTECȚIA INFRASTRUCTURILOR CRITICE

Dr. Claudia LASCATEU
Manager superior de securitate cibernetică,
Directoratul Național de Securitate Cibernetică, București
Drd. Mihai CONSTANTINESCU
Manager superior de securitate cibernetică,
Directoratul Național de Securitate Cibernetică, București
10.55535/GMR.2024.4.17

The integration of robust cybersecurity tools and technologies within healthcare institutions is a critical strategy for strengthening national security and enhancing deterrence, particularly within NATO framework. This article highlights the strategic importance in mitigating targeted cyber threats.

Critical tools for real-time threat detection, establishing secure network perimeters, and comprehensive network security are discussed for their efficacy in pre-empting and responding to sophisticated cyber-attacks. Additionally, the strategic outsourcing of cybersecurity services to specialized third-party providers is explored, demonstrating the enhanced defence mechanisms achieved through leveraging external expertise and advanced technologies.

The article underscores the necessity of a multi-faceted cybersecurity approach, analysing the strategy and policy applied to the unique demands of the healthcare sector. By enhancing the cybersecurity posture of healthcare institutions, this research posits a significant increase in national preparedness against targeted cyber threats.

Keywords: national security; cyber security; healthcare system; advanced technologies; NATO;

INTRODUCERE

Creșterea dependenței de tehnologiile digitale în sectoarele critice, precum sănătatea, a adus în prim-plan importanța unei securități cibernetice robuste ca pilon al securității naționale. Într-o lume interconectată, amenințările cibernetice care vizează infrastructura medicală au devenit o preocupare majoră atât pentru sistemele de sănătate publică, cât și pentru mecanismele naționale de apărare. Această vulnerabilitate în creștere a impus integrarea unor măsuri sofisticate de securitate cibernetică, menite să reducă riscurile asociate atacurilor cibernetice, în special cele orchestrate de actori statali și non-statali.

Acest articol își propune să analizeze rolul soluțiilor avansate de securitate cibernetică în consolidarea securității naționale în sectorul sănătății, cu un accent deosebit pe abordarea strategică a României, evidențiată în *Strategia de securitate cibernetică* adoptată prin HG nr. 1321/2021 și aprobată în 2022. Într-un context geopolitic mai larg, aceste măsuri se aliniază cadrului defensiv al NATO, care prioritizează interoperabilitatea și reziliența infrastructurii în fața amenințărilor cibernetice complexe.

Explorarea detaliată a tehnologiilor, cum ar fi inteligența artificială (AI) pentru detecția amenințărilor, protecția end-point și criptarea avansată a datelor, demonstrează cum aceste soluții nu doar asigură confidențialitatea, integritatea și disponibilitatea datelor sensibile din sănătate, dar contribuie și la o strategie de descurajare. Aceasta este în concordanță cu postura de apărare colectivă a NATO, care recunoaște faptul că perturbarea sistemelor de sănătate critice ar putea avea efecte în lanț asupra stabilității naționale și a securității internaționale. Mai mult, prin prisma Manualului Tallinn 2.0 și a Dreptului internațional umanitar (DIU), protecția infrastructurilor medicale în timpul conflictelor cibernetice devine o obligație legală, accentuând necesitatea unor capabilități defensive avansate.

Prin adoptarea unei abordări multi-fațetate în securitatea cibernetică, România își propune să își consolideze reziliența în fața amenințărilor cibernetice din ce în ce mai sofisticate, întărind, astfel, arhitectura de securitate nu doar la nivel național, ci și în rândul aliaților NATO. Acest articol subliniază imperativul de a îmbina inovația tehnologică cu colaborarea strategică, atât la nivel național,

cât și internațional, pentru a proteja infrastructurile medicale de atacuri cibernetice sofisticate, asigurând, astfel, securitatea națională și siguranța publică. Printr-o analiză a politicilor existente, a cadrelor juridice și a tehnologiilor avansate, acest studiu oferă perspective asupra viitorului apărării cibernetice în sectorul sănătății ca element central în cadrul securității naționale și internaționale.

ROLUL INFRASTRUCTURII MEDICALE ÎN SECURITATEA NAȚIONALĂ ȘI ÎN CADRUL NATO

Sistemul de sănătate, prin digitalizarea sa accelerată, a devenit parte integrantă a infrastructurii critice naționale, necesară pentru asigurarea securității publice și a stabilității sociale. În cadrul *Strategiei de securitate cibernetică* a României, protejarea acestor infrastructuri este esențială pentru securitatea națională și pentru apărarea împotriva atacurilor cibernetice.

NATO recunoaște importanța infrastructurilor critice pentru menținerea stabilității naționale și regionale. Un atac asupra sistemelor de sănătate nu doar că afectează furnizarea serviciilor esențiale, ci creează vulnerabilități care pot fi exploatate în scopuri de destabilizare politică și militară.

Sistemul național de securitate cibernetică prevede protecția sectorului sănătății prin implementarea unor măsuri specifice, precum evaluarea vulnerabilităților, prevenirea incidentelor și intervenția rapidă în cazul atacurilor cibernetice.

Infrastructura medicală și securitatea națională

Importanța infrastructurii medicale depășește sfera sănătății publice, având un impact direct asupra securității naționale și a stabilității sociale. Protecția infrastructurii medicale împotriva atacurilor cibernetice este esențială nu doar pentru continuitatea serviciilor, ci și pentru prevenirea exploatării vulnerabilităților de către actori statali sau non-statali, inclusiv în situații de conflict.

Conform *Strategiei de securitate cibernetică* a României, infrastructurile critice, inclusiv sectorul sănătății, sunt esențiale pentru securitatea națională, necesitând măsuri de protecție cibernetică specializate. În acest context, respectarea prevederilor Dreptului internațional umanitar (DIU) și ale Manualului Tallinn 2.0 este crucială pentru abordarea atacurilor cibernetice asupra infrastructurii critice în mod compatibil cu dreptul internațional.

Protecția infrastructurilor medicale în cadrul NATO din perspectiva Dreptului internațional umanitar și a Manualului Tallinn 2.0

NATO recunoaște protecția infrastructurilor critice ca un element esențial pentru menținerea stabilității naționale și regionale. Atacurile cibernetice asupra sistemelor medicale sunt considerate o amenințare semnificativă, având potențialul de a destabiliza nu doar furnizarea de servicii esențiale, dar și echilibrul politic și militar într-un stat membru al NATO.

În conformitate cu Manualul Tallinn 2.0, infrastructurile medicale sunt protejate în mod explicit împotriva atacurilor cibernetice în situații de conflict. Manualul prevede că atacurile asupra sistemelor informatice medicale sunt interzise, întrucât acestea nu reprezintă ținte militare legitime și sunt protejate de **principiul distincției**. Astfel, distrugerea sau perturbarea intenționată a serviciilor medicale, fie prin mijloace cibernetice sau fizice, poate fi considerată o încălcare a dreptului internațional umanitar.

Articolul 99 din Manualul Tallinn 2.0 subliniază faptul că unitățile medicale și alte infrastructuri care oferă îngrijiri sunt protejate de la a fi ținte legitime în conflicte armate cibernetice, iar statele au obligația de a lua măsuri adecvate pentru a proteja aceste obiective împotriva atacurilor cibernetice.

Sistemul național de securitate cibernetică și protecția sectorului sănătății

România, prin sistemul național de securitate cibernetică, implementează măsuri concrete pentru protejarea infrastructurilor critice, inclusiv sectorul sănătății. Aceste măsuri sunt aliniate cu dreptul internațional umanitar și cu principiile enunțate în Manualul Tallinn 2.0, care consideră că infrastructurile medicale trebuie protejate atât în timp de pace, cât și în timpul conflictelor armate cibernetice.

În conformitate cu Manualul Tallinn 2.0, România trebuie să adopte măsuri preventive, cum ar fi:

- Evaluarea vulnerabilităților cibernetice ale infrastructurilor medicale și îmbunătățirea securității pentru a preveni atacuri cibernetice de amploare.
- Prevenirea incidentelor prin implementarea unor soluții avansate de securitate, cum ar fi detectarea intruziunilor (IDS/IPS), criptarea datelor și monitorizarea în timp real a sistemelor.
- Intervenția rapidă în caz de atacuri cibernetice prin echipe specializate, conform prevederilor DIU și ale Manualului Tallinn 2.0, care subliniază necesitatea unui răspuns coordonat și proporțional în caz de atac.

Impactul atacurilor cibernetice asupra securității naționale și regionale conform Dreptului internațional umanitar și Manualului Tallinn 2.0

Atacurile cibernetice asupra infrastructurii medicale pot perturba grav funcționarea sistemului de sănătate, dar au și un impact semnificativ asupra lanțului de aprovizionare (supply chain) al sectorului medical, ceea ce poate cauza consecințe grave asupra securității naționale și regionale. În acest context, DIU și Manualul Tallinn 2.0 oferă un cadru solid pentru protejarea nu doar a infrastructurilor medicale, ci și a sistemelor asociate lanțului de aprovizionare cibernetic. În conformitate cu **principiul proporționalității** din dreptul conflictelor armate, statele trebuie să se abțină de la atacuri care pot cauza daune disproporționate infrastructurilor civile, inclusiv celor medicale. Manualul Tallinn 2.0 consolidează aceste principii, evidențiind că orice atac asupra unui spital sau a unui sistem informatic medical poate constitui o încălcare gravă a DIU și poate fi considerat o violare a DIU.

Lanțul de aprovizionare medicală cuprinde o rețea complexă de sisteme, care includ producția, stocarea și distribuția de medicamente, echipamente medicale și alte materiale critice necesare pentru funcționarea eficientă a serviciilor de sănătate. În era digitală, această rețea se bazează puternic pe infrastructuri informatice pentru gestionarea comenzilor, transportului și monitorizării stocurilor. În conformitate cu Manualul Tallinn 2.0, un atac cibernetic asupra infrastructurii de sănătate poate afecta grav lanțul de aprovizionare, cu efecte colaterale majore, cum ar fi lipsa de echipamente medicale esențiale sau medicamente pentru populație.

Articolul 70 din Manualul Tallinn 2.0 stabilește că atacurile cibernetice trebuie să fie direcționate numai către ținte militare și nu pot include unități medicale sau sistemele informatice asociate acestora. În plus, infrastructurile medicale trebuie protejate **împotriva atacurilor indirecte sau a efectelor colaterale ale operațiunilor cibernetice**.

Atacurile cibernetice care perturbă supply chain-ul medical pot avea consecințe devastatoare asupra funcționării sistemului de sănătate și asupra securității naționale. În timpul pandemiei COVID-19, am fost martori la vulnerabilitățile lanțurilor de aprovizionare, unde orice întârziere în livrarea echipamentelor medicale sau a medicamentelor esențiale a avut un impact direct asupra sănătății publice. Într-un conflict cibernetic, perturbarea acestor lanțuri poate fi folosită ca tactică de destabilizare, ducând la o criză sanitară și socială de proporții.

Dreptul internațional umanitar prevede protecția nu doar a infrastructurilor medicale, ci și a rețelelor critice care susțin aceste infrastructuri. Manualul Tallinn

2.0 extinde această protecție la rețelele digitale care gestionează logistica și aprovizionarea cu resurse medicale, subliniind faptul că atacurile asupra acestor rețele reprezintă o violare a principiului proporționalității din DIU. Un atac cibernetic care afectează lanțul de aprovizionare al unui spital, blocând furnizarea de echipamente sau medicamente esențiale, ar putea cauza un efect disproporționat asupra populației civile și ar putea fi considerat o crimă de război.

NATO a recunoscut **vulnerabilitatea lanțurilor de aprovizionare cibernetice** și a stabilit măsuri de protecție a infrastructurilor critice care sprijină aprovizionarea medicală și logistica în caz de conflict. În cadrul strategiilor de apărare cibernetică, NATO promovează partajarea de informații între statele membre pentru identificarea și prevenirea vulnerabilităților din lanțurile de aprovizionare. În plus, NATO încurajează colaborarea între sectorul public și privat pentru a securiza aceste rețele critice.

România, în calitate de membru al NATO, este obligată să adopte măsuri pentru protecția supply chain-ului medical și a infrastructurilor care susțin aprovizionarea cu resurse esențiale. În contextul unei amenințări cibernetice, protecția acestor rețele este esențială pentru a asigura continuitatea serviciilor medicale și pentru a preveni o criză majoră de sănătate publică.

Conform Dreptului internațional umanitar și prevederilor din Manualul Tallinn 2.0, statele au obligația de a lua măsuri proactive pentru a proteja infrastructurile critice, inclusiv lanțurile de aprovizionare medicală, împotriva atacurilor cibernetice (Articolul 99 din Manualul Tallinn 2.0).

Dreptul internațional umanitar și Manualul Tallinn 2.0

Atacurile cibernetice sunt recunoscute ca forme moderne de conflict, iar Manualul Tallinn 2.0 oferă un cadru juridic esențial pentru abordarea acestora în conformitate cu dreptul conflictelor armate. Infrastructurile medicale, în special cele digitalizate, sunt protejate nu doar de normele tradiționale ale DIU, dar și de noile interpretări și ghiduri oferite de Manualul Tallinn 2.0, care afirmă că atacurile cibernetice asupra infrastructurilor medicale sunt interzise, indiferent de forma conflictului, care la Articolul 99 interzice atacurile care vizează sistemele informatice ce gestionează infrastructura medicală, precum și lanțurile de aprovizionare medicală. Atacurile cibernetice care duc la perturbarea serviciilor medicale și a infrastructurii asociate pot fi considerate crime de război, în conformitate cu normele DIU.

*

Infrastructura medicală este un pilon critic în securitatea națională și internațională, iar protecția sa în fața atacurilor cibernetice este reglementată atât de DIU, cât și de Manualul Tallinn 2.0. Aceste cadre juridice oferă protecție explicită unităților medicale, interzicând orice atac cibernetic care ar putea perturba funcționarea acestora.

România, în colaborare cu NATO și aliniată la prevederile Manualului Tallinn 2.0, are responsabilitatea de a implementa măsuri proactive pentru protejarea infrastructurilor medicale împotriva atacurilor cibernetice. Măsurile de securitate cibernetică și strategiile naționale trebuie să fie în concordanță cu prevederile DIU și ale Manualului Tallinn 2.0 pentru a asigura respectarea obligațiilor internaționale și a proteja aceste infrastructuri esențiale în timpul conflictelor cibernetice.

AMENINȚĂRI CIBERNETICE ȘI NECESITATEA UNEI ABORDĂRI INTEGRATE

România, ca parte a unei regiuni din ce în ce mai expuse la atacuri cibernetice de amploare, a dezvoltat *Strategia de securitate cibernetică* pentru a proteja infrastructurile critice, cum este sectorul sănătății, de amenințările cibernetice provenite de la actori statali și non-statali. Acest capitol analizează necesitatea unei abordări integrate pentru protecția sectorului sănătății în lumina reglementărilor și cadrelor internaționale relevante, inclusiv Directiva NIS2, Dreptul internațional umanitar, Manualul Tallinn 2.0, Legea securității cibernetice nr. 58/2023, precum și măsurile incluse în raportul Inventory.

Amenințări cibernetice și relevanța Directivei NIS2

Directiva NIS2 (Network and Information Security Directive), adoptată la nivelul Uniunii Europene, reprezintă un cadru legislativ esențial pentru protecția infrastructurilor critice, inclusiv a sectorului sănătății, împotriva amenințărilor cibernetice. Directiva pune accent pe confidențialitatea, integritatea și disponibilitatea datelor, având ca scop îmbunătățirea securității și rezilienței infrastructurilor critice la nivel național și european.

În contextul NIS2, sectorul sănătății este definit ca o infrastructură esențială, iar România, în calitate de stat membru al UE, trebuie să implementeze măsuri de securitate cibernetică robuste pentru a se alinia la cerințele europene. Printre acestea se numără:

- Audituri de securitate regulate pentru evaluarea riscurilor cibernetice.

- Măsuri de răspuns rapid în cazul incidentelor de securitate cibernetică.
- Sisteme de detecție și prevenție a atacurilor cibernetice avansate.

NIS2 cere implementarea de soluții tehnologice avansate, cum ar fi inteligența artificială și blockchain, pentru a asigura securitatea datelor medicale și a infrastructurilor critice de sănătate.

Legea securității cibernetice nr. 58/2023 și aplicarea sa în sectorul sănătății

Legea securității cibernetice nr. 58/2023 oferă un cadru legislativ național care se aliniază la cerințele Directivei NIS2 și stabilește obligații clare pentru protecția infrastructurilor critice, inclusiv a celor din sectorul sănătății. Această lege introduce măsuri stricte de protecție a datelor și de gestionare a incidentelor de securitate, cerând entităților din sectorul medical să implementeze măsuri de securitate tehnică și organizațională pentru a preveni atacurile cibernetice și pentru a reacționa prompt la acestea.

Legea nr. 58/2023 impune:

- Obligativitatea raportării incidentelor cibernetice care afectează infrastructurile critice, inclusiv sistemele informatice din domeniul sănătății.
- Partajarea de informații între sectorul public și privat pentru a identifica și a neutraliza rapid amenințările cibernetice.

Această lege se alătură altor reglementări internaționale, cum ar fi Manualul Tallinn 2.0 și DIU, pentru a asigura protecția infrastructurii medicale împotriva atacurilor cibernetice, în conformitate cu standardele internaționale de securitate.

Raportul RO-CCH și implementarea tehnologiilor emergente

Conform Raportului *Inventory of cyber security tools and technologies suitable for or dedicated to healthcare and health institutions(D4.3)* din Proiectul Romanian Cyber Care Health – RO-CCH (RO-CCH, 2022), finanțat de Comisia Europeană prin CNECT.H – Digital Society, Trust, and Cybersecurity, România a început să implementeze o serie de măsuri avansate pentru consolidarea capacității de apărare cibernetică, cu accent pe protecția infrastructurilor critice din domeniul sănătății. Raportul subliniază importanța utilizării tehnologiilor emergente, cum ar fi:

- Inteligența artificială (AI) pentru detecția în timp real a amenințărilor.
- Blockchain pentru securizarea datelor medicale și a lanțurilor de aprovizionare.
- Criptarea avansată pentru protecția datelor sensibile împotriva interceptării neautorizate.

Aceste tehnologii sunt esențiale pentru a răspunde la amenințările complexe și evolutive, venite din partea actorilor statali și non-statali. De asemenea, raportul RO-CCH menționat recomandă efectuarea de audituri regulate și utilizarea unor platforme de gestionare a incidentelor pentru a asigura continuitatea operațională a serviciilor medicale în fața unor potențiale atacuri cibernetice.

Necesitatea unei abordări integrate

România, prin *Strategia de securitate cibernetică*, face pași importanți în protejarea infrastructurilor critice, dar trebuie să continue să adopte măsuri eficiente în cooperare cu partenerii săi internaționali, precum NATO și Uniunea Europeană. Colaborarea interinstituțională și transmiterea de informații între sectorul public și privat sunt cruciale pentru crearea unui mediu cibernetic rezilient.

În plus, abordarea integrată trebuie să includă și măsuri de educare și conștientizare a personalului medical și IT cu privire la noile amenințări și tehnologii. Manualul Tallinn 2.0, DIU, NIS2 și Legea nr. 58/2023 oferă un cadru solid pentru securizarea infrastructurilor medicale, dar implementarea acestor reglementări la nivel național și local este esențială pentru protecția sectorului sănătății în fața amenințărilor cibernetice.

*

România a dezvoltat un cadru robust pentru protecția infrastructurilor critice, inclusiv a sectorului sănătății, prin intermediul *Strategiei de securitate cibernetică*, Directivei NIS2, Legii nr. 58/2023 și principiilor stabilite în Manualul Tallinn 2.0 și în Dreptul internațional umanitar. Aceste măsuri sunt esențiale pentru asigurarea confidențialității, integrității și disponibilității datelor medicale, dar și pentru protecția infrastructurilor medicale împotriva atacurilor cibernetice susținute de actori statali și non-statali. România trebuie să continue să investească în tehnologii avansate, să efectueze audituri de securitate periodice și să consolideze cooperarea internațională pentru a crea un mediu cibernetic rezilient și sigur.

MĂSURI AVANSATE DE SECURITATE CIBERNETICĂ ÎN SECTORUL SĂNĂTĂȚII ȘI IMPACTUL LOR ASUPRA SECURITĂȚII NAȚIONALE ȘI A STRATEGIEI NATO

Strategia de securitate cibernetică a României, prevăzută în HG nr. 1321/2021 și aprobată în 2022, promovează utilizarea tehnologiilor inovatoare, cum ar fi inteligența artificială și sistemele de analiză comportamentală, pentru a îmbunătăți

capacitățile de detecție și răspuns în sectorul sănătății. Conform HG nr. 1321/2021, este esențial ca infrastructurile de sănătate să fie protejate prin măsuri tehnologice avansate, cum ar fi firewall-uri de generație nouă, sisteme de monitorizare continuă a traficului și programe de prevenție a pierderii datelor. Aceste măsuri sunt necesare pentru a proteja datele pacienților și a preveni atacuri cibernetice ce pot destabiliza infrastructura medicală.

În cadrul strategiei NATO, interoperabilitatea și securitatea infrastructurii sunt priorități cheie. Utilizarea acestor tehnologii în România contribuie la întărirea securității cibernetice în domeniul sănătății și la asigurarea unei defensive cibernetice robuste, compatibile cu cerințele NATO.

Politici și strategii naționale

Strategia de securitate cibernetică a României constituie fundamentul politicilor naționale în protecția infrastructurii critice, inclusiv a sectorului sănătății. Aceasta promovează utilizarea de tehnologii inovatoare pentru a întări capacitățile de detecție și răspuns în fața amenințărilor cibernetice, subliniind necesitatea adoptării soluțiilor de securitate avansate, precum:

- Sistemele de analiză comportamentală, care ajută la identificarea activităților cibernetice anormale și pot detecta atacurile înainte ca acestea să provoace daune semnificative.

Conform HG nr. 1321/2021, infrastructurile de sănătate sunt considerate critice pentru securitatea națională, iar protecția acestora este esențială pentru prevenirea atacurilor cibernetice ce ar putea destabiliza întreaga infrastructură medicală. Măsurile tehnologice promovate în această strategie includ:

- Firewall-uri de generație nouă pentru protecția perimetrului rețelei.
- Sisteme de monitorizare continuă a traficului pentru a detecta activități suspecte.
- Programe de prevenție a pierderii datelor (DLP), care protejează datele sensibile ale pacienților de la sustragere sau distrugere.

Aceste măsuri avansate contribuie la asigurarea confidențialității, integrității și disponibilității datelor pacienților și reprezintă o barieră importantă împotriva atacurilor cibernetice ce vizează destabilizarea infrastructurilor medicale.

Interoperabilitatea și strategiile NATO

În cadrul strategiei NATO, securitatea cibernetică a infrastructurilor critice, inclusiv a sectorului sănătății, este considerată **o prioritate de securitate colectivă**. România, ca stat membru al NATO, își aliniază politicile naționale cu cerințele

Alianței, asigurând interoperabilitatea și capacitatea de a reacționa unitar la atacurile cibernetice. NATO subliniază importanța interoperabilității între sistemele cibernetice ale statelor membre pentru a asigura un răspuns rapid și eficient la atacurile coordonate de actori statali și non-statali.

Printre măsurile tehnologice și tactice promovate de NATO pentru protecția infrastructurilor medicale se numără:

- Sisteme de management al incidentelor (SIEM), care integrează date din diferite surse și ajută la detectarea și gestionarea incidentelor cibernetice.
- Soluții avansate de protecție end-point, pentru a asigura securitatea dispozitivelor conectate la rețea.
- Platforme de prevenire a pierderilor de date (DLP), menite să prevină scurgerea de date sensibile sau accesul neautorizat la informații esențiale pentru securitatea națională și sănătatea publică.

Aceste măsuri sunt esențiale pentru a preveni atacuri precum ransomware sau alte tipuri de atacuri complexe care vizează nu doar datele medicale, ci și funcționarea critică a sistemelor informatice din sectorul sănătății. Interoperabilitatea dintre aceste sisteme este crucială pentru a asigura o apărare cibernetică robustă și compatibilă cu standardele NATO, consolidând, astfel, apărarea colectivă a infrastructurilor critice din regiune.

Impactul măsurilor avansate asupra securității naționale și internaționale

Adoptarea măsurilor avansate de securitate cibernetică în sectorul sănătății are un impact profund asupra securității naționale și internaționale, contribuind la stabilitatea infrastructurilor critice și la apărarea împotriva atacurilor cibernetice. Această secțiune analizează implicațiile acestor măsuri din perspectiva teoriei descurajării cibernetice, a conformității cu normele internaționale și a rolului lor în consolidarea capacităților naționale de apărare cibernetică, potrivit *Strategiei de securitate cibernetică* a României, Manualului Tallinn 2.0 și Dreptului internațional umanitar.

Impactul asupra securității naționale

Măsurile avansate de securitate cibernetică au o influență directă asupra securității naționale, în special prin protecția infrastructurii critice de sănătate. Potrivit teoriei rezilienței cibernetice, capacitatea unei națiuni de a rezista și de a răspunde rapid la amenințările cibernetice asigură continuitatea funcționării serviciilor esențiale. Protecția sistemelor informatice care gestionează datele

pacienților și fluxurile de aprovizionare medicală contribuie la stabilitatea internă și la menținerea ordinii publice, chiar și în situații de atac cibernetic de amploare.

În conformitate cu *Strategia de securitate cibernetică* a României, măsurile precum utilizarea inteligenței artificiale (AI) pentru detecția și răspunsul la incidente, implementarea de firewall-uri de generație nouă și sisteme de prevenție a pierderilor de date (DLP) reprezintă instrumente cheie pentru prevenirea și gestionarea atacurilor cibernetice asupra infrastructurii medicale. Aceste tehnologii sunt esențiale pentru a preveni compromiterea confidențialității, integrității și disponibilității datelor medicale și pentru a proteja resursele critice necesare funcționării sistemelor de sănătate.

Conform teoriei apărării cibernetice pro-active, utilizarea unor tehnologii precum AI nu doar că ajută la detecția în timp real a amenințărilor, dar permite și o reacție anticipată la atacuri, minimizând impactul asupra infrastructurii critice. Implementarea acestor măsuri contribuie la asigurarea continuității operaționale, un obiectiv central al securității naționale în orice criză de securitate cibernetică.

Impactul asupra securității internaționale și cooperarea cu NATO

La nivel internațional, integrarea măsurilor de securitate avansate conform standardelor NATO contribuie la întărirea securității colective și la conformitatea cu cerințele strategiei de apărare cibernetică a Alianței. Interoperabilitatea dintre sistemele cibernetice naționale și cele ale aliaților din NATO este esențială pentru a asigura o apărare robustă și coordonată împotriva amenințărilor cibernetice. Conform teoriei securității colective, capacitatea de a răspunde rapid și eficient la atacuri cibernetice contribuie la descurajarea actorilor statali și non-statali care ar putea încerca să exploateze vulnerabilitățile în infrastructurile medicale.

Tehnologiile precum SIEM (Security Information and Event Management), firewall-urile avansate și protecția end-point asigură detectarea și gestionarea rapidă a incidentelor, permițând României să acționeze în cadrul strategiilor NATO și să contribuie la stabilitatea regională. Utilizarea AI și a analizelor comportamentale ajută la prevenirea atacurilor sofisticate și la reducerea timpului de răspuns, întărind, astfel, capacitatea de apărare cibernetică la nivel internațional.

Efectul disuasiv asupra actorilor malițioși

Un alt aspect esențial al măsurilor avansate de securitate cibernetică este efectul disuasiv pe care acestea îl au asupra actorilor malițioși. *Teoria descurajării*

cibernetice[1] sugerează că prezența unor tehnologii avansate, combinate cu capacitatea statului de a detecta și a răspunde rapid la atacuri, creează un mediu cibernetic mai puțin favorabil pentru atacatori. România, prin adoptarea acestor măsuri, își întărește capacitatea de descurajare la nivel național și internațional, făcând dificilă compromiterea infrastructurilor medicale.

Firewall-urile de generație nouă și DLP joacă un rol esențial în protejarea infrastructurilor medicale de la sustragerea sau compromiterea datelor sensibile. Conform teoriei disuasiunii prin negare, măsurile avansate de securitate cibernetică sporesc costurile și riscurile pentru atacatori, reducând, astfel, probabilitatea unor atacuri reușite.

Protecția infrastructurilor medicale conform Manualului Tallinn 2.0 și Dreptului internațional umanitar

În contextul Manualului Tallinn 2.0 și Dreptului internațional umanitar, măsurile avansate de securitate cibernetică asigură protecția juridică a infrastructurilor medicale în cazul conflictelor cibernetice. Măsurile avansate de securitate cibernetică implementate în România asigură conformitatea cu aceste norme internaționale, reducând riscurile de încălcare a principiului distincției. Prin protejarea infrastructurilor medicale de atacuri cibernetice, România își îndeplinește obligațiile internaționale și contribuie la menținerea stabilității și securității globale în fața conflictelor cibernetice.

Măsurile avansate de securitate cibernetică implementate în sectorul sănătății, prevăzute în HG nr. 1321/2021 și susținute de strategia NATO, au un impact semnificativ asupra securității naționale și internaționale. Utilizarea tehnologiilor de ultimă generație, cum ar fi AI și criptarea avansată, precum și aplicarea unor politici și strategii naționale și internaționale, contribuie la întărirea rezilienței infrastructurilor critice și la protejarea cetățenilor împotriva atacurilor cibernetice.

[1] Teoria descurajării poate fi examinată mai detaliat prin distingerea între două concepte cheie: descurajarea prin negare și descurajarea prin pedeapsă. Descurajarea prin negare presupune prevenirea adversarilor de a-și atinge obiectivele, făcând atacurile dificile sau improbabile, de obicei prin măsuri defensive solide, cum ar fi sisteme avansate de securitate cibernetică, criptare și detectarea în timp real a amenințărilor. În schimb, descurajarea prin pedeapsă se concentrează pe impunerea unor consecințe semnificative sau represalii asupra atacatorilor, descurajându-i să inițieze atacuri din cauza riscurilor ridicate implicate. În domeniul securității cibernetice, ambele strategii pot fi aplicate: negarea prin măsuri tehnice care fac sistemele greu de compromis și pedeapsa prin măsuri legale și diplomatice. În sectorul sănătății, descurajarea prin pedeapsă poate lua forma răspunsurilor legale și diplomatice la atacurile cibernetice care vizează infrastructurile medicale, inclusiv colaborarea cu aliați internaționali pentru a izola actorii malițioși (N.A.).

Alinierea cu politicile NATO, adoptarea măsurilor din Directiva NIS2 și respectarea normelor din Manualul Tallinn 2.0 asigură o protecție robustă și integrată a sectorului sănătății. Aceste măsuri întăresc apărarea cibernetică la nivel național și internațional, contribuind la stabilitatea și securitatea regiunii și la protecția infrastructurilor critice în fața unor amenințări tot mai complexe.

CONSOLIDAREA SECURITĂȚII NAȚIONALE ȘI INTERNAȚIONALE ÎN SISTEMELE DE SĂNĂTATE

Analizând impactul măsurilor avansate de securitate cibernetică asupra securității naționale și internaționale, vom evidenția câteva dintre teoriile aplicate în sectorul sănătății, precum: *Defense in Depth, „Zero Trust", „Deterrence by Denial", „Cyber Resilience"și „Shared Responsibility".*

Teoriile menționate subliniază nevoia unui cadru integrat, care să includă măsuri tehnologice avansate, colaborare interinstituțională și parteneriate internaționale pentru a asigura protecția eficientă a infrastructurilor critice. Prin aplicarea acestor cadre teoretice, considerăm că România poate contribui la întărirea securității sale naționale și regionale, menținându-se în conformitate cu normele internaționale și aliniindu-se cu standardele NATO și ale UE în materie de securitate cibernetică.

Teoria „Defense in Depth" și aplicarea acesteia în sectorul sănătății

Teoria apărării în profunzime *(Defense in Depth)* este un concept esențial în securitatea cibernetică și promovează ideea că securitatea eficientă se bazează pe mai multe straturi de apărare. În contextul securității cibernetice a sectorului sănătății, această abordare este aplicată prin utilizarea unei combinații de tehnologii, proceduri și măsuri organizaționale pentru a proteja infrastructura critică.

Măsurile tehnologice avansate, cum ar fi firewall-urile de generație nouă, criptarea datelor și protecția end-point, sunt doar un strat din acest sistem multi-nivel. Implementarea sistemelor de prevenire a pierderilor de date (DLP), a platformelor SIEM și a soluțiilor de detecție comportamentală constituie alte straturi de apărare, creând o barieră rezistentă în fața atacurilor cibernetice.

Această teorie susține că reducerea dependenței de un singur mecanism de protecție și crearea unei arhitecturi cu mai multe niveluri de securitate ajută la întârzierea și detectarea atacurilor cibernetice, reducând, astfel, riscurile de succes ale acestora. În sectorul sănătății, aplicarea teoriei *„Defense in Depth"* contribuie la protecția în adâncime a datelor sensibile și a funcționalităților critice, sporind gradul de reziliență a sistemului.

Teoria „Zero Trust” și protecția datelor medicale

Teoria *„Zero Trust”* a devenit o paradigmă centrală în securitatea cibernetică modernă. Aceasta presupune că nu trebuie să existe încredere implicită între diferite segmente ale rețelei sau între utilizatorii care accesează resursele. Într-un sistem *„Zero Trust”*, accesul la resurse este oferit doar pe baza verificărilor continue ale identității și conformității cu politicile de securitate.

În sectorul sănătății, această teorie se aplică prin controlul strict al accesului la datele medicale și la infrastructurile esențiale. Fiecare accesare este monitorizată și verificată, eliminând riscul ca un atacator să obțină acces neautorizat și să sustragă sau să compromită datele critice. Criptarea datelor și utilizarea autentificării multi-factor (MFA) sunt elemente centrale ale implementării acestei teorii.

Adoptarea modelului *„Zero Trust”* în infrastructurile de sănătate contribuie la crearea unui mediu cibernetic mai sigur și reduce semnificativ riscul de atacuri interne sau externe care ar putea compromite datele pacienților. În context internațional, acest model este esențial pentru asigurarea interoperabilității și a protecției datelor sensibile între partenerii din cadrul NATO și al UE.

Teoria „Deterrence by Denial” și descurajarea cibernetică

Teoria *„Deterrence by Denial”* este o abordare care se concentrează pe prevenirea succesului unui atac prin măsuri tehnice și organizaționale care fac atacurile extrem de dificil de realizat. În cazul sectorului sănătății, aplicarea acestei teorii constă în dezvoltarea unor sisteme cibernetice reziliente, astfel încât atacatorii să fie descurajați din start, datorită complexității și eficienței măsurilor de securitate implementate.

Măsurile avansate de securitate cibernetică, cum ar fi detecția în timp real a anomaliilor, monitorizarea continuă și utilizarea soluțiilor de răspuns automatizat la incidente cibernetice, sunt instrumente care contribuie la *deterrence by denial*. Un exemplu clar este implementarea tehnologiilor AI pentru analiza comportamentală care poate detecta și răspunde proactiv la atacuri înainte ca acestea să devină o amenințare majoră.

În acest context, capacitatea statului de a preveni succesul atacurilor cibernetice asupra infrastructurilor de sănătate creează un scut de descurajare care protejează atât securitatea națională, cât și pe cea internațională. Această teorie se aliniază și cu *Teoria apărării active*, care presupune monitorizarea și intervenția continuă pentru prevenirea activităților malițioase.

Teoria „Cyber Resilience” și importanța capacităților de recuperare

Teoria *„Cyber Resilience”* este esențială pentru înțelegerea impactului măsurilor avansate de securitate cibernetică asupra securității naționale și internaționale. Reziliența cibernetică se referă la capacitatea unei infrastructuri critice de a detecta, a rezista și a se recupera rapid în urma unui atac cibernetic, asigurând continuitatea operațiunilor esențiale.

În sectorul sănătății, aceasta înseamnă că nu doar măsurile de prevenție și detecție sunt importante, ci și capacitatea sistemelor de a reveni la o stare operațională normală după un incident cibernetic. Implementarea unor planuri de recuperare în caz de dezastru (DRP) și a sistemelor de backup sunt elemente centrale ale acestei teorii, care completează strategiile de securitate cibernetică avansată.

Capacitățile de reziliență sunt esențiale în cadrul colaborării internaționale, deoarece atacurile cibernetice pot afecta simultan infrastructuri din mai multe țări. Capacitatea României de a colabora eficient cu partenerii săi din NATO și din UE pentru a asigura continuitatea operațională a infrastructurilor de sănătate este un pilon central în strategia sa de securitate cibernetică.

Teoria „Shared Responsibility” și colaborarea între stat și sectorul privat

Un alt cadru teoretic relevant pentru analiza impactului măsurilor avansate de securitate cibernetică este teoria *„Shared Responsibility”* (responsabilitate comună). Aceasta sugerează că securitatea cibernetică a infrastructurilor critice, cum este sectorul sănătății, nu poate fi asigurată doar de stat, ci necesită o colaborare strânsă între sectorul public și cel privat.

În acest context, statul creează cadrul legislativ și infrastructura de bază pentru securitatea cibernetică, dar entitățile private – cum ar fi furnizorii de servicii medicale și companiile de tehnologie – joacă un rol crucial în implementarea și menținerea măsurilor de securitate. Acest parteneriat între stat și sectorul privat este esențial pentru a asigura continuitatea și reziliența infrastructurii medicale împotriva amenințărilor cibernetice.

Legea nr. 58/2023 impune acest principiu prin solicitarea ca entitățile care operează infrastructuri critice să colaboreze cu autoritățile naționale pentru protejarea sistemelor lor, în conformitate cu cerințele internaționale.

CONCLUZII

Pe măsură ce atacurile cibernetice devin mai sofisticate și mai frecvente, viitoarele direcții de cercetare în domeniul securității cibernetice pentru infrastructurile critice, inclusiv sectorul sănătății, ar trebui să exploreze mai multe domenii cheie care să sprijine continuarea evoluției măsurilor de protecție și apărare.

Prin implementarea *Strategiei de securitate cibernetică* a României și adoptarea unei poziții coerente cu standardele NATO și cerințele Directivei NIS2, România își consolidează capacitățile de apărare cibernetică. Aceste măsuri nu doar protejează infrastructurile critice de sănătate împotriva atacurilor cibernetice, dar creează și un efect disuasiv semnificativ asupra actorilor statali și non-statali care ar încerca să exploateze vulnerabilitățile digitale.

Totodată, aplicarea principiilor Dreptului internațional umanitar și a normelor din Manualul Tallinn 2.0 subliniază necesitatea protejării infrastructurilor medicale în contextul conflictelor cibernetice, asigurând conformitatea României cu legislația internațională privind protecția civililor și a infrastructurilor esențiale. Acest cadru legal oferă o bază solidă pentru protecția infrastructurilor critice de sănătate și contribuie la menținerea stabilității naționale și regionale.

În concluzie, apreciem că securitatea cibernetică avansată în sectorul sănătății este o componentă indispensabilă a securității naționale și internaționale, iar aplicarea unor tehnologii inovatoare, alături de respectarea normelor internaționale, constituie o strategie eficientă pentru protejarea împotriva amenințărilor cibernetice. Prin colaborarea cu partenerii internaționali și prin implementarea unor măsuri de securitate robuste, România își consolidează poziția de lider în securitatea cibernetică regională și contribuie la reziliența colectivă a NATO și a Uniunii Europene. Această abordare holistică asigură protecția cetățenilor și a infrastructurilor critice în fața provocărilor complexe ale spațiului cibernetic modern.

BIBLIOGRAFIE:

1. *Dreptul internațional umanitar și Protecția infrastructurilor civile*, https://www.icrc.org/en/document, accesat la 12 iunie 2024.
2. *EU Cyber Resilience Act*, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52022PC0454, accesat la 23 mai 2024.
3. Hotărârea de Guvern nr. 1.321 din 30 decembrie 2021, prin care a fost aprobată *Strategia de securitate cibernetică a României pentru perioada 2022-2027*, precum și *Planul de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027*, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128, accesat la 13 august 2024.
4. *Inventory of cyber security tools and technologies suitable for or dedicated to healthcare and health institutions (D4.3) "Romanian Cyber Care Health – RO-CCH"*, RO-CCH - DIGITAL-2022-CYBER-02, https://dnsc.ro/pagini/proiect-ro-cch, accesat la 22 mai 2024.
5. *Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, https://legislatie.just.ro/Public/DetaliiDocument/265677, accesat la 2 iunie 2024.
6. *NATO's Concept for Deterrence and Defence*, https://www.nato.int/docu/review/articles/2021, accesat la 22 mai 2024.
7. *NATO Cyber Defence Policy*, https://www.nato.int/cps/en/natolive/topics_78170.htm., accesat la 22 iunie 2024.
8. RO-CCH (2022), https://dnsc.ro/pagini/proiect-ro-cch, accesat la 14 iunie 2024.
9. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, https://ccdcoe.org/research/tallinn-manual, accesat la 23 mai 2024.