APĂRARE CIBERNETICĂ, TEHNOLOGII DISRUPTIVE ȘI REZILIENȚĂ ÎN SECOLUL XXI

General de brigadă Mihai BURLACU
Șeful Direcției Comunicații și Tehnologia Informației

Într-o eră în care competiția tehnologică pare că a devenit mai acerbă ca niciodată, spațiul cibernetic reprezintă tot mai mult unul dintre principalii vectori de tip Smart Power pentru inițierea și ducerea acțiunilor ostile. Suntem, în prezent, parte a unei societăți globale, în care Tehnologia a schimbat radical comportamentul și așteptările noastre zilnice în privința accesului la informații sau la servicii digitale. Totodată, Transformarea digitală reprezintă calea prin care ne adaptăm sistemic la cerințele operațiilor militare contemporane. Faptul că atacurile de tip cibernetic au devenit un fenomen cotidian, fie că vorbim de mediul economic, social sau militar, confirmă cât de puternică a devenit influența asimetrică, integrată cibernetic, în mediul nostru de apărare și securitate.

Când, la nivelul NATO, s-au abordat pentru prima dată capabilitățile cibernetice, în anul 2002, din perspectiva vulnerabilităților și riscurilor mediului informațional, s-au avut în vedere mai degrabă un set de cerințe de ordin tehnic, simțindu-se nevoia dezvoltării de tip hard a instrumentelor puterii militare prin adoptarea și integrarea componentei cibernetice în zona operațională. În prezent, spațiul cibernetic a devenit esențial pentru angajarea strategică în materie de descurajare și apărare. Continuitatea succesului politic și militar al Alianței și abilitatea acesteia de a îndeplini sarcinile sale principale se bazează din ce în ce mai mult pe adoptarea rapidă a tehnologiilor digitale. Avantajele obținute și menținute la scara NATO sunt estimate a fi în pericol spre anii 2030,

dacă nu se adoptă acțiuni imediate în statele membre pentru păstrarea acestei superiorități tehnologice, contestată prin eforturile și energia competitorilor strategici și a potențialilor adversari de sorginte autocratică. Acestea solicită, din partea Aliaților, investiții semnificative în dezvoltarea și integrarea noilor capabilități digitale. În acest fel, Transformarea digitală a NATO va permite Alianței să desfășoare operații integrate multidomeniu/MDO, să consolideze interoperabilitatea între toate domeniile operaționale, să optimizeze avertizările, capacitatea de alertă și răspuns la diferite tipuri de amenințări, să faciliteze consultările politice și procesul de luare a deciziei bazat pe date/informații relevante. Astfel, în foarte mare măsură, dependențele de spațiul cibernetic conjugat cu cel fizic, electromagnetic, ca mediu operațional, devin critice pentru viitoarele confruntări sau acțiuni militare.

Această evoluție a importanței domeniului cyber a fost marcată de câteva evenimente importante, cum ar fi: recunoașterea, de către aliați, a apărării cibernetice ca parte a misiunii de bază a NATO de apărare colectivă în 2014, reconsiderarea spațiului cibernetic drept domeniu al operațiilor în 2016 și, cel mai recent, o nouă politică de apărare cibernetică la nivelul NATO, în 2021.

Spațiul cibernetic este un domeniu unic, în care tehnologiile, inclusiv cele emergente și disruptive, joacă un rol extrem de important. Respectivele tehnologii pot genera atât oportunități, pentru cei în situația de a se apăra în spațiul cibernetic, cât și vulnerabilități, ce pot fi exploatate de atacatori. În acest sens, analiza realizată de Comandamentul Aliat pentru Transformare al NATO cu privire la spațiul cibernetic – Cyberspace Strategic Foresight Analysis – evidențiază faptul că potențialii competitori și adversari vor include, într-o măsură din ce în ce mai mare, operațiile din acest domeniu în propriile strategii de ducere a războiului, cu precădere pentru a răspunde la operațiile de tip hibrid sau informaționale. Astfel, luând în considerare progresele tehnologice anticipate pentru următorii zece ani, este foarte probabil ca actorii scenei internaționale, entități statale și non-statale, să-și optimizeze capabilitățile relative la atacuri cibernetice.

Mai mult, documentul menționat identifică tehnologiile emergente și disruptive relevante, fie ca amenințare, fie ca oportunitate, după cum urmează: inteligența artificială, tehnologiile cuantice, comunicațiile 5G, expansiunea orașelor inteligente, cloud, blockchain, Software Defined Radios și Zero Trust Networks. În acest sens, sunt sugerate și modalități de răspuns, fiind încurajată adoptarea unui nou tip de abordare a diferitelor tehnologii la mai multe niveluri, în funcție de stadiul de dezvoltare a acestora – embrionare, incipiente, mature, ce pot fi exploatate de statele membre ale NATO, dar și de potențialii adversari, respectiv tehnologii deja existente în NATO. Între modalitățile de răspuns sugerate, articulate pe cele patru niveluri, sunt menționate următoarele: observarea și monitorizarea, cercetarea și experimentarea, adoptarea și implementarea imediate, respectiv menținerea și optimizarea programelor existente.

Este evident faptul că puterea oferită de domeniul cibernetic conferă mijloace de influență pentru stat și actori nestatali, deopotrivă. Dar, limitele respectivei puteri sunt în permanentă evaluare, așa cum sunt și conceptele cheie ale NATO.

Există, în prezent, dezbateri active dacă noțiunea de „descurajare cibernetică" se aplică la fel ca în cazul domeniilor tradiționale (terestru, aerian, maritim și spațial). Cyberspațiul este contestat în mod constant, la niveluri diferite, făcându-l un domeniu în care descurajarea sau apărarea împotriva oricărei activități ostile este aproape imposibil de anticipat și extrem de dificil de realizat.

Cu toate acestea, ca parte a apărării colective, conform misiunilor de bază ale Alianței, un atac cibernetic grav asupra unui aliat ar putea fi tratat ca un atac asupra tuturor și, ca atare, ar putea declanșa articolul 5 din Tratatul Atlanticului de Nord. Nu există praguri predefinite privind răspunsul în cazul unui astfel de atac. NATO trebuie să-și consolideze mandatul defensiv din această perspectivă, astfel încât să fie gata să răspundă unui atac cibernetic chiar și atunci când articolul 5 nu este invocat. La fel și în cazul tuturor membrilor luați individual..., fiecare, în parte, trebuie să-și dezvolte infrastructura astfel încât să poată face față și răspunde unei astfel de provocări.

În acest scop, NATO poate servi drept platformă de conectare și diseminare a lecțiilor învățate între aliați, facilitând politica de consultare și de inițiere a unor acțiuni colective ca răspuns la atacurile cibernetice. Spațiul cibernetic este adesea exploatat de adversari în scopul dezinformării și propagandei – forme de amenințări hibride, de tip soft power, care complică și mai mult mediul de securitate, întrucât sunt menite să submineze societățile din interior prin influențarea deciziilor la nivel instituțional. Prin urmare, menținerea avantajului competitiv, într-o lume în care normele și legile internaționale care guvernează spațiul cibernetic sunt contestate neîncetat, este mai crucială ca oricând.

Războiul din Ucraina a confirmat că Federația Rusă este capabilă și foarte activă în spațiul cibernetic, apelând la întregul spectru de atacuri și acțiuni distructive în urmărirea obiectivelor sale strategice, cu mai mică sau mai mare intensitate, atât în perioada premergătoare conflictului, cât și în susținerea demonstrativă sau complementar acțiunilor cinetice. Rusia a pregătit cu grijă terenul de confruntare cibernetic, asigurându-și din timp accesul la rețelele și infrastructurile critice. Pe întreaga durată a crizei și conflictului, Rusia a exploatat acele vulnerabilități identificate anterior ca parte a unei campanii cibernetice coordonate, ce a inclus tactici de exfiltrare, dar și un număr fără precedent de variante de malware distructiv. Acestea au avut efecte multiplicative, fiind propagate în afara Ucrainei, inclusiv în statele membre ale NATO (e.g. prejudicierea serviciilor Viasat), evidențiind determinarea Rusiei de a accepta riscuri cu consecințe imprevizibile în cascadă.

Deși reziliența rămâne o responsabilitate națională, aliații NATO au analizat o serie de cerințe de bază, pe care fiecare stat le poate folosi pentru a-și evalua nivelurile de reziliență. Cerințele se referă la servicii publice vitale, inclusiv aprovizionarea cu energie, transport și rețele de telecomunicații, asistență medicală, infrastructură critică, alimente și resursele de apă – toate componentele fiind necesare atât pentru managementul integrat al crizei, cât și pentru sprijinirea operațiilor de apărare. De asemenea, asigurarea securității rețelelor de telecomunicații de ultimă generație va deveni și mai importantă odată

cu integrarea rețelelor 5G, deoarece acestea devin fundamentul ecosistemelor de tehnologii existente și al altora noi, care pot transforma radical conceptul de securitate. Pe măsură ce și mai multe dintre dispozitivele și interacțiunile noastre sunt digitalizate, legătura dintre spațiul cibernetic și tehnologiile emergente și disruptive (emerging and disruptive technologies – EDTs) se va extinde. Cu alte cuvinte, noi căi pentru a perturba societățile și ordinea internațională bazată pe reguli. Așadar, regulile și normele trebuie adaptate pentru ca societățile să poată face față schimbării mediului strategic prin raportare la dezvoltările tehnologice.

În România, postura de descurajare și apărare împotriva unor agresiuni cibernetice concertate, ce vizează infrastructurile critice naționale, impune un nivel mai înalt de cooperare interinstituțională, în special la nivelul Centrelor de operații cibernetice și al entităților implicate în managementul incidentelor, o cooperare susținută și structurată cu sectorul privat, care solicită o angajare bazată pe parteneriate public-privat stabilite pe termen lung și o integrare superioară a eforturilor de înțelegere comună asupra situației în spațiul cibernetic la nivel politic, militar și tehnic. O postură activă de descurajare în spațiul cibernetic necesită și pregătirea unor capabilități care să fie în măsură să producă efecte în rețelele și infrastructurile critice ale potențialilor adversari, bazată pe o forță digitală gata să intervină în spațiul cibernetic, înalt calificată, motivată și încurajată printr-o schimbare culturală asertivă și un leadership adecvat, care poate recunoaște performanța și calitățile inovative, susține experimentarea în exploatarea și managementul integrat al datelor, precum și dezvoltarea capacității de asumare a unui risc calculat și bine informat.

În concluzie, progresul tehnologic poate avea implicații militare majore, ce țin de schimbarea naturii războiului și a caracterului conflictelor. Drept urmare, este de așteptat ca operațiile viitoare ale Alianței să se desfășoare într-un cadru complet diferit de cel tradițional. Implementarea și dezvoltarea continuă a celui de-al cincilea mediu operațional, reprezentat de mediul cibernetic, favorizează apariția unor noi centre de putere ale căror obiective se pot intercala pe diferite domenii de interes și pot conduce la noi situații conflictuale atât în mediul real, cât și în cel virtual. Nu în ultimul rând, mediul cibernetic reprezintă vectorul modern de proiectare a condițiilor necesar a fi îndeplinite în scopul obținerii unui nivel superior de Smart Power, raportat la specificitatea provocărilor realității cotidiene actuale.

Astfel, pentru a putea răspunde adecvat amenințărilor din domeniul tehnologic, este necesar ca factorii de decizie din domeniul securității și apărării să se concentreze asupra activităților de dezvoltare a capabilităților și de planificare a operațiilor la cele trei niveluri – strategic, operațional și tactic, pe termen mediu și lung. România, alături de celelalte state membre ale Alianței, implementează măsurile aferente, astfel încât să contribuie la efortul de apărare colectivă, precum și la postura de apărare și descurajare a NATO, cu precădere în flancul estic, unde se situează și Regiunea Extinsă a Mării Negre, cu particularitățile sale, generate, în primul rând, de poziția sa geostrategică, și conștientizând, totodată, efectele impactului tehnologic asupra confruntărilor din spațiul cibernetic.