REPUBLICA POPULARĂ CHINEZĂ ȘI AMENINȚĂRILE LA ADRESA SECURITĂȚII CIBERNETICE A NATO

Căpitan-comandor drd. Claudiu-Cosmin RADU
Universitatea Națională de Apărare „Carol I", București
10.55535/GMR.2024.4.16

In recent years, many NATO member states have reported violations of cyber sovereignty, accusing the People's Republic of China (PRC). PRC has its own vision of cyberspace, employing technological advances to strengthen its position as a global leader. This article addresses NATO's cyber security challenges, analysing how Beijing's actions influence international politics and cyber stability. Utilizing a combination of qualitative and quantitative analysis, the research explores the ways in which the PRC pursues its geopolitical goals in cyberspace, as well as NATO's response measures. From the analysis of cyber security policies, we draw insights into the strategic directions each side is pursuing. The article also assesses the long-term impact of cyber tensions between the PRC and NATO and exposes the importance of international collaboration in promoting a stable and secure cyberspace. The conclusions emphasize the need for a coordinated and proactive approach to counter cyber threats and strengthen the Alliance's cyber defence.

Keywords: People's Republic of China; cyber security; NATO; cyber threats; cyberspace;

INTRODUCERE

Progresul accelerat al tehnologiei informațiilor și comunicațiilor din ultimii ani a avut o importanță însemnată în dezvoltarea capabilităților cibernetice la nivel mondial. Odată cu avansul tehnologic, Republica Populară Chineză, denumită în continuare RPC, a devenit o forță importantă, nu doar pe plan economic și militar, ci și în spațiul cibernetic, consolidându-și prezența în acest domeniu esențial pentru securitatea internațională. În contextul acestor evoluții, NATO, alianța formată din statele democratice occidentale, se confruntă cu provocări fără precedent, generate de acțiunile cibernetice agresive din spațiul cibernetic. În viziunea statelor membre, principalele țări care finanțează actori non-statali sau conduc activități cibernetice ofensive sunt considerate Federația Rusă, Republica Populară Chineză, Coreea de Nord și Iran (Diotte, 2020).

Expansiunea RPC în spațiul cibernetic a atras atenția marilor puteri occidentale, în special a Statelor Unite ale Americii, care consideră Beijingul principala amenințare în ceea ce privește securitatea cibernetică. Potrivit unor rapoarte ale NATO și ale altor organizații internaționale, RPC a dezvoltat strategii complexe de spionaj cibernetic, utilizând metode sofisticate de infiltrare și colectare de informații pentru a obține avantaje economice, militare și geopolitice (Hamilton, 2020). RPC își manifestă tot mai mult influența în spațiul cibernetic prin politici și strategii special gândite și adaptate pentru a obține suveranitate în spațiul cibernetic. Concepția sa asupra acestui domeniu operațional este apreciată drept inovatoare și de perspectivă, deoarece consideră spațiul cibernetic ca pe o extensie virtuală a teritoriului, pe care încearcă să o controleze în același mod în care își gestionează teritoriul fizic . Această abordare generează provocări deosebite pentru Alianța Nord-Atlantică, care promovează un spațiu cibernetic liber, deschis, pașnic și sigur și depune eforturi pentru a spori stabilitatea și a reduce fricțiunile între țări. Aceste obiective se doresc a fi realizate prin intermediul dreptului internațional și ale normelor acceptate privind comportamentul responsabil al statelor în spațiul cibernetic (NATO, 2024).

Strategia cibernetică a RPC vizează în special acțiuni de descurajare și coerciție în spațiul cibernetic (Hamilton, ib.), unde Beijingul duce acțiuni ofensive împotriva entităților guvernamentale și a infrastructurilor critice ale adversarilor săi, inclusiv state membre ale NATO. Această tactică face parte dintr-o strategie mai amplă

de influență geopolitică, prin care RPC urmărește să își extindă prezența și să își consolideze statutul de putere mondială. Activitățile cibernetice intense ale RPC reprezintă una dintre principalele preocupări pentru NATO, datorită complexității și frecvenței ridicate a atacurilor cibernetice lansate. Aceste atacuri variază de la atacuri DDoS (Distributed Denial of Service) la infiltrări sofisticate în rețelele guvernamentale, civile sau chiar militare, având ca scop vulnerabilizarea rețelelor și obținerea de informații critice pentru securitatea națională. Marea provocare pentru NATO este de a-și întări apărarea împotriva acestor atacuri cibernetice din ce în ce mai avansate. În acest context, Alianța a implementat inițiative pentru a stimula coordonarea și cooperarea între statele membre în domeniul securității cibernetice. Totuși, progresele rapide ale RPC în tehnologii de vârf, precum inteligența artificială și quantum computing, amplifică complexitatea acestui peisaj, determinând NATO să își intensifice eforturile pentru a dezvolta tehnici mai eficiente de contracarare.

Scopul principal al prezentului este de a analiza evoluția și activitățile cibernetice ale RPC și impactul acestora asupra securității Alianței-Nord Atlantice. În acest context, obiectivele propuse sunt: analizarea tacticilor și scopurilor utilizate de RPC în spațiul cibernetic și corelarea răspunsurilor Alianței-Nord Atlantice pentru a contracara amenințările RPC în acest mediu. Mai mult, lucrarea își propune să analizeze și implicațiile pe termen lung ale acestui conflict cibernetic și modul în care alianțele internaționale pot juca un rol decisiv în menținerea securității globale în era digitală.

Metodologia cercetării constă preponderent din metode de tip calitativ, dar include și unele metode cantitative prin analiza de conținut a legilor, strategiilor și politicilor care guvernează spațiul cibernetic din RPC și NATO, precum și a literaturii de specialitate. Pornind de la această analiză, studiul de față își propune să răspundă la următoarea întrebare de cercetare: *Este NATO pregătit pentru a contracara în mod eficient acțiunile tot mai sofisticate din spațiul cibernetic inițiate de RPC?*

Analiza de conținut a politicilor cibernetice ale administrației de la Beijing subliniază intenția acesteia de a utiliza spațiul cibernetic în scopul realizării ambițiilor sale geopolitice, economice și de securitate națională. O strategie care integrează avansul tehnologic cu un control intern riguros, suveranitatea cibernetică și controlul informațional sunt esențiale pentru Beijing atât pentru menținerea stabilității interne, cât și pentru extinderea influenței sale globale. În același timp, capacitatea RPC de a dezvolta și utiliza ofensiv tehnologii avansate prezintă riscuri semnificative pentru securitatea cibernetică globală, impunând necesitatea unui răspuns coordonat din partea NATO și a partenerilor săi.

EVOLUȚIA ȘI PERSPECTIVELE POLITICILOR CIBERNETICE ALE REPUBLICII POPULARE CHINEZE

Pentru a înțelege acțiunile RPC în spațiul cibernetic, este esențial să analizăm câteva dintre motivațiile și scopurile care stau la baza acestor acțiuni. Acest demers nu urmărește să justifice comportamentul RPC, ci să ofere o perspectivă asupra factorilor ce influențează deciziile și strategiile adoptate. După sfârșitul Războiului Rece, perioadă în care existau practic două mari centre de putere, s-au conturat noi actori internaționali dornici să-și afirme autoritatea în diverse domenii. Pe măsură ce aceste noi puteri și-au afirmat influența, multe dintre ele, inclusiv RPC, au cunoscut o ascensiune rapidă în domenii precum tehnologia, economia și puterea militară. RPC, cu ambiții evidente de a deveni un actor important în economia mondială, a investit masiv în dezvoltarea tehnologiilor avansate, având în vedere dorința de a-și consolida influența geopolitică și de a reduce dependența de alte state. Această competiție globală, alimentată cu orgoliile și ambițiile politice ale liderilor chinezi, a determinat un ritm accelerat de cercetare și inovare în tehnologii emergente, precum inteligența artificială, tehnologia 5G și 6G, Internet of Things (IoT) și quantum computing. În acest context, RPC a recunoscut rapid valoarea și potențialul spațiului cibernetic nu doar ca mediu pentru dezvoltare economică, ci și ca un domeniu strategic pentru obținerea unui avantaj competitiv asupra altor state, fie prin spionaj cibernetic, fie prin furt de proprietate intelectuală, fie prin atacuri asupra infrastructurilor critice (Chafetz, 2023). Aceste acțiuni sunt motivate de dorința RPC de a-și extinde influența globală, de a-și proteja interesele economice și de a se poziționa ca un lider tehnologic internațional. Prin această abordare agresivă pornită de la nivel politico-administrativ, Beijingul urmărește nu doar să își afirme supremația în spațiul cibernetic, ci și să își consolideze rolul de putere globală, capabilă să influențeze ordinea internațională și să se impună într-un peisaj geopolitic tot mai competitiv. Aceste acțiuni sunt profund înrădăcinate în structura autocratică a statului, care favorizează controlul centralizat și subordonarea intereselor economice și juridice în favoarea Partidului Comunist.

În ultimul deceniu, competiția generală dintre Republica Populară Chineză și Statele Unite s-a intensificat semnificativ, iar un nou front al acestei rivalități s-a conturat în spațiul cibernetic. În acest context, ambele state se acuză reciproc de spionaj cibernetic, practici de concurență neloială și imixtiuni în infrastructurile critice naționale. Infrastructura critică, ce include rețelele de energie electrică, sistemele de transport și comunicațiile, reprezintă un obiectiv deosebit de sensibil la nivel național, iar securitatea acestor sisteme este esențială pentru funcționarea

oricărei națiuni moderne. În plus, intruziunea în aceste rețele este percepută ca o amenințare la adresa securității naționale, fiind tratată de majoritatea statelor în strategiile naționale și strategiile de securitate cibernetică.

O mare parte a tensiunii din spațiul cibernetic dintre RPC și SUA se concentrează pe acuzațiile de spionaj, atât în sfera militară, cât și în cea economică. Deși ambele națiuni se acuză reciproc de spionaj extins, această practică nu este limitată la cele două state. Majoritatea statelor membre ale NATO au experimentat o gamă mai extinsă de incidente cibernetice din partea unor actori statali sau non-statali care au avut legături cu RPC. În mod paradoxal, complexitatea și interdependențele economice dintre state determină o anumită prudență în desfășurarea unor astfel de acțiuni. Cu toate acestea, competiția continuă să fie dusă prin atacuri de tip DDoS, infiltrări în rețelele unor instituții guvernamentale și campanii de influențare prin dezinformare, toate acestea încadrându-se în limitele războiului hibrid. Cu toate acestea, atacurile cibernetice sunt adesea considerate o componentă a strategiei diplomatice și militare contemporane, fără a escalada pragul care ar declanșa conflicte armate directe (Jinghua, 2019).

Începând cu anii 1990, RPC a început să înțeleagă impactul profund pe care noile tehnologii le-ar putea avea asupra viitorului. Oficialii de la Beijing au intuit potențialul dezvoltării capabilităților cibernetice, în primul rând pentru costurile sale reduse, și în al doilea rând pentru eficiența cu care puteau înlocui tehnologiile convenționale. Rețelele de internet au fost puse sub un control strict, deoarece conducerea a fost preocupată de controlul accesului la internet și infrastructură digitală. Existau temeri că țara ar putea deveni vulnerabilă la atacuri din partea altor națiuni, care începuseră deja să integreze soluții digitale avansate în strategiile lor militare (Jiang, T., 2022).

Această perioadă a fost una de consolidare, fiind influențată de conflictele militare în care s-au utilizat tehnologii avansate pentru acea vreme în conflicte precum Războiul din Golf, din 1991, care a servit drept o demonstrație clară a avantajului tehnologic american. Acest conflict este considerat de mulți analiști ca fiind primul *„război informatizat”*, datorită utilizării intensive a tehnologiilor moderne, cum ar fi sisteme avansate de comunicații, radare, sateliți și arme ghidate. În esență, s-au folosit tehnici de război electronic pentru a perturba și intercepta comunicațiile irakiene, precum și pentru a coordona cu precizie atacurile. Deși nu s-au lansat atacuri cibernetice propriu-zise, războiul a demonstrat dependența crescândă de tehnologiile informatice în război, ceea ce a prefigurat importanța acțiunilor din spațiul cibernetic în conflictele viitoare. Cu toate acestea, abia în 1999, în timpul

conflictului din Kosovo, au fost utilizate atacuri cibernetice, fiind caracterizat drept primul *„război pe internet”*. Actorii guvernamentali și neguvernamentali deopotrivă au folosit internetul pentru a disemina informații, a răspândi propagandă, știrile false și a solicita sprijin pentru pozițiile lor (Denning, 2001). Urmare a evenimentelor petrecute la nivel mondial, RPC a perceput necesitatea de a-și accelera propriile capacități cibernetice, ca măsură preventivă. În același timp, se pun bazele consolidării controlului asupra infrastructurilor cibernetice naționale din RPC. Ambiția de securitate în spațiul cibernetic este puternic influențată de modul în care s-a desfășurat strategia de informatizare a RPC. În anul 2000, aceasta și-a stabilit obiectivul de a deveni o societate informațională avansată, în care întreprinderile, oamenii de știință și cetățenii utilizează cele mai moderne tehnologii ale informației și comunicațiilor (TIC) pentru a îmbunătăți performanța și a spori beneficiile sociale (Austin, 2018, p. 11).

La nivel național s-au intensificat cercetările și dezvoltarea în domeniul cibernetic cu scopul de a-și securiza teritoriul împotriva amenințărilor externe. Mai mult decât atât, strategia Beijingului se concentrează puternic pe *„suveranitatea rețelei”*, ceea ce se traduce prin abilitatea Guvernului de a controla fluxul de informații din internet. Aceasta a inclus implementarea unor măsuri stricte de cenzură și monitorizare a traficului de date, menite să împiedice infiltrările externe și să protejeze interesele naționale (Jiang, T., ib.). Potrivit aceluiași autor, începând cu anul 2008, RPC a devenit cea mai mare piață de internet din lume, având peste 253 de milioane de utilizatori. Această expansiune rapidă a internetului a coincis cu ascensiunea sa pe podiumul economic mondial. Însă, dezvoltarea internetului nu a fost doar un motor de creștere a economiei, ci și o sursă de vulnerabilități, devenind tot mai atentă la pericolele asociate securității cibernetice. Înainte de toate, statul a început să conștientizeze necesitatea de a-și proteja infrastructurile critice, precum instituțiile financiare și rețelele energetice, împotriva potențialelor amenințări venite din spațiul cibernetic. La fel ca majoritatea statelor, RPC depinde semnificativ de tehnologie, ceea ce face ca Guvernul să urmărească îndeaproape evoluțiile legate de internet și de fluxul de informații pe care acesta le generează. Autoritățile chineze percep informațiile necontrolate ca o amenințare la adresa regimului și depun eforturi considerabile pentru a beneficia de oportunitățile economice oferite de internet, menținând, totodată, controlul politic asupra acestuia (Grauman, 2012).

În acest context, Partidul Comunist Chinez a perceput internetul ca pe o amenințare la adresa stabilității regimului, având în vedere impactul posibil al influențelor externe asupra populației chineze. Pentru a combate aceste riscuri,

RPC a început în 1998 să dezvolte o strategie bazată pe supravegherea și restricționarea accesului la informații. Un prim pas esențial în acest sens a fost lansarea, în 2003, a *Proiectului Golden Shield*, care reprezintă baza *„Marelui Firewall" a RPC.* Acest proiect permite regimului să cenzureze conținutul online și să blocheze accesul la sursele de informații străine, considerate dăunătoare sau subversive. Prin acest proiect se dorește filtrarea și controlul traficului de internet, blocând accesul la conținutul din afara granițelor țării, considerat sensibil (Austin, p. 11), izolând efectiv internetul național de internetul global. Cu alte cuvinte, autoritățile combină cenzura digitală cu supravegherea socială, ceea ce le permite să urmărească și să controleze comportamentul online al cetățenilor. Ca parte a acestui proiect, începând din 2009, RPC a depus eforturi pentru a bloca anumite aplicații software din SUA (precum Facebook, Twitter și YouTube) din cauza incompatibilității acestora cu legile sale privind cenzura (The International Institute for Strategic Studies, 2021).

Pentru a asigura conformitatea cu reglementările în vigoare, proiectul integrează și măsuri de identificare digitală prin care cetățenii sunt obligați să folosească numele reale pe platformele online, ca obiectiv al menținerii securității cibernetice (Triolo, Sacks, 2017). Astfel, utilizatorii devin direct responsabili pentru activitățile lor online, reducând posibilitatea disidenței anonime și sporind autocenzura. Mai mult decât atât, *Golden Shield* a devenit, astfel, un pilon central în strategia cibernetică a RPC, stabilind standarde pentru controlul informațiilor și cenzura internetului. Acesta marchează un aspect fundamental al politicilor mai largi ale RPC în materie de securitate cibernetică și suveranitate informațională, stabilind un model de internet controlat de stat care se aliniază strâns cu prioritățile de securitate națională. Acest cadru este esențial pentru înțelegerea dezvoltării și punerii în aplicare a politicilor cibernetice chinezești în viitor.

După anul 2007, au avut loc mai multe evenimente în spațiul cibernetic. Rusia a fost acuzată că a folosit spațiul cibernetic pentru acțiuni ofensive împotriva Estoniei și a Georgiei, iar SUA că ar fi în spatele atacului cu Stuxnet. Mai mult decât atât, revoltele din timpul Primăverii Arabe au evidențiat pentru RPC importanța consolidării propriilor capacități cibernetice pentru a-și proteja infrastructurile critice și a menține stabilitatea națională. Incidentul Stuxnet a demonstrat vulnerabilitățile rețelelor industriale la atacuri sofisticate, determinând RPC să reevalueze strategiile cibernetice pentru a preveni astfel de amenințări. În această perioadă, SUA au recunoscut spațiul cibernetic ca un nou domeniu de operațional, pe lângă cele terestru, aerian, maritim și spațial (The White House, 2011). Această recunoaștere a accentuat atenția Beijingului asupra dezvoltării tehnologiilor, în vederea protejării

intereselor naționale și a menținerii securității interne într-un peisaj global tot mai complex. Drept urmare, în această perioadă, pe măsură ce RPC a devenit a doua cea mai mare economie din lume, dezvoltarea politică, economică și socială a acesteia a fost puternic integrată în spațiul cibernetic la nivel global (Jiang, T., ib.).

În 2010, RPC a publicat o Carte Albă privind statutul IoT, subliniind necesitatea securității cibernetice pentru a proteja securitatea națională și interesele statului pe teritoriul său suveran (Hwang, 2023), fapt care relevă recunoașterea importanței securității cibernetice în contextul securității naționale. Un an mai târziu, RPC împreună cu alte state, printre care Rusia, Tadjikistan și Uzbekistan, au prezentat în Adunarea Generală a ONU un *Cod Internațional de Conduită privind Securitatea Informațiilor (International Code of Conduct for Information Security).* Acesta a reafirmat convingerea că drepturile și responsabilitățile decizionale pentru politicile publice legate de internet ar trebui să se afle sub jurisdicția statului gazdă (United Nations General Assembly, 2011).

O nouă etapă în securitatea cibernetică a RPC a fost deschisă atunci când președintele țării, Xi Jinping, a anunțat intenția țării de a deveni o putere cibernetică. El a inițiat o serie de schimbări instituționale pentru a contribui la realizarea acestui obiectiv. Una dintre cele mai importante a fost crearea Administrației Chineze a Spațiului Cibernetic (Cyberspace Administration of China/CAC) în cursul anului 2014. Această instituție devine responsabilă de reglementarea, administrarea și licențierea internetului din RPC. Punctul de vedere oficial din RPC, la fel ca în majoritatea țărilor bogate și cu venituri medii, este că securitatea cibernetică afectează și modelează întreaga gamă de activități guvernamentale, economice, sociale, tehnologice, politice și de securitate din țară (Austin, p. 7).

În anul 2015, s-a înființat Centrul de Evaluare a Securității Tehnologiei Informației din China (China Information Technology Security Evaluation Center), sub comanda CAC, cu rol în consolidarea apărării naționale împotriva amenințărilor cibernetice. Prin activitatea sa de cercetare, centrul a oferit perspective esențiale și strategii pentru protejarea eficientă a RPC în fața atacurilor cibernetice (Jiang, T., ib.). Tot în același an, Guvernul a publicat noi reglementări, vizând companiile IT străine care aprovizionează băncile chinezești, impunându-le să dezvăluie codurile sursă ale produselor IT furnizate. Măsura a fost impusă pentru a consolida atât securitatea cibernetică internă, cât și localizarea industriei de securitate cibernetică (Austin, p. 14). Răspunsul a venit pe linie politico-diplomatică atunci când relațiile bilaterale RPC-SUA s-au răcit, determinând RPC să suspende măsurile tot în același an.

Pe măsură ce internetul și tehnologiile cibernetice au devenit o parte esențială a economiei și securității naționale, strategia RPC a evoluat de la control și ofensivă la apărare și descurajare. În acest context, Beijingul și-a ajustat politicile pentru a face față atât provocărilor interne, cât și celor externe, concentrându-se pe prevenirea atacurilor cibernetice și pe protejarea infrastructurilor sale critice. Ascensiunea sa ca superputere cibernetică a fost marcată de o tranziție de la expansiune agresivă la protecție strategică, odată cu integrarea tot mai profundă în economia globală. Începând cu 2015, RPC a început să adopte o poziție mai defensivă în ceea ce privește strategia sa cibernetică. Dacă, în primele etape, strategia era concentrată pe atacuri preemtive și pe consolidarea suveranității cibernetice, treptat, atenția s-a mutat către apărare și descurajare (Jiang, T., 2019). Această schimbare reflectă o conștientizare tot mai mare a riscurilor unui război cibernetic la scară largă și a costurilor economice și politice asociate acestuia (Soesanto, 2022).

Pe plan politic, actuala administrație chineză a recunoscut pe deplin importanța securității cibernetice și a declarat-o parte a securității naționale. Drept urmare, a emis mai multe legi și strategii naționale pentru a consolida capacitățile de apărare cibernetică ale țării. Astfel, *Legea privind securitatea națională a Republicii Populare Chineze,* din anul 2015, oferă cadrul general pentru securitatea națională și securitatea cibernetică (Jiang, M., 2020). Mai mult decât atât, articolul 25 din *Legea Securității Naționale* accentuează importanța dezvoltării științifice, inovării și control național asupra tehnologiilor informaționale de bază, infrastructurilor critice, sistemelor și datelor informatice importante. De asemenea, stabilește obiective de prevenire, oprire și gestionare a atacurilor cibernetice, intruziunilor în rețele, furtului informatic, distribuirii online de informații compromițătoare, ducând, în cele din urmă, la obținerea securității și suveranității în spațiul cibernetic. În ceea ce privește strategiile cibernetice publicate de Administrația Chineză a Spațiului Cibernetic, *Strategia Internațională de Cooperare în Spațiul Cibernetic,* aprobată în 2016, se remarcă datorită faptului că RPC iese în evidență prin faptul încearcă să preia conducerea guvernanței cibernetice internaționale, ca urmare a apelului președintelui Xi de a *„stabili o comunitate a viitorului comun în spațiul cibernetic”* (Jiang, M., ib.). Această strategie subliniază în mod deosebit principiile păcii, suveranității, guvernanței partajate și susține pacea prin cooperare și încrederea strategică reciprocă.

Pe plan național, mai multe instituții au adoptat legi sau au emis politici privind protecția datelor cu caracter personal, regulamente administrative sau reguli privind activitățile informaționale din spațiul cibernetic. În ceea ce privește

activitatea infracțională, Dreptul Penal al Chinei a fost revizuit de mai multe ori, în anii 2005, 2009 și 2015, pentru a reflecta creșterea activităților infracționale care implică informații personale. *Legea Securității Cibernetice* a RPC din anul 2017 conține, în mod similar, câteva dispoziții care reglementează colectarea, stocarea, transmiterea și utilizarea *„informațiilor cu caracter personal”* de către operatorii de rețea și operatorii de infrastructură informatică critică (Jiang, M., ib.). Această lege a fost creată pentru a proteja infrastructura rețelelor naționale și pentru a controla activitățile companiilor străine în spațiul cibernetic chinez. Legea cere companiilor să implementeze standarde stricte de securitate și să raporteze informații privind vulnerabilitățile din rețelele lor către autorități. Putem afirma faptul că această lege reiterează conceptul de suveranitate cibernetică ca instrument de securitate națională.

În ceea ce privește spațiul cibernetic ca domeniu operațional, administrația de la Beijing a publicat, în 2019, Cartea Albă – *Apărarea națională a Chinei în noua eră*. Aceasta expune o evaluare a situației actuale a securității naționale și internaționale și prezintă misiunile, reformele și cheltuielile RPC în domeniul apărării. Acest document oferă o analiză detaliată a stării actuale a securității naționale și internaționale, descriind misiunile, reformele și cheltuielile RPC în sectorul apărării. Mai mult, se subliniază necesitatea ca armata chineză să se adapteze *„noii ere”* a competiției strategice prin îmbunătățirea pregătirii și creșterea capacităților de luptă, aliniindu-se, astfel, cu statutul global al RPC, dar și cu angajamentul său pentru menținerea *„păcii mondiale”*. În domeniul apărării cibernetice, Cartea Albă evidențiază interesul Beijingului pentru adoptarea celor mai avansate tehnologii în sectorul militar, inclusiv inteligența artificială, big data, cloud computing, quantum computing și internetul obiectelor (IoT) (The State Council Information Office of the People's Republic of China, 2019). În plus, programul de modernizare militară presupune o strategie de *„fuziune civil-militară”*, consolidând relațiile companiilor civile cu instituțiile de apărare. Prin această fuziune, armata chineză ar putea beneficia de progresele tehnologice din multe domenii, precum tehnologia nucleară, aerospațială, aviația, semiconductorii, cloud computing, robotica și prelucrarea *„Big Data”* (Ford, 2019).

Similar cu alte state, RPC își propune să domine spațiul cibernetic, recunoscând, totodată, necesitatea unei transformări substanțiale a forțelor sale armate pentru a atinge acest scop strategic. Președintele Xi Jinping și echipa sa au pus bazele unei transformări a Armatei Populare de Eliberare (APL) într-o *„armată de clasă*

mondială", până în 2050. Realizarea aceasta depinde de capacitatea statului de a adapta tehnologiile emergente și inteligența artificială la doctrina militară existentă (Burke, Gunness, Cooper III, Coza, 2020). În continuare, autorii expun faptul că Directivele strategice ale APL evidențiază importanța spațiului cibernetic ca domeniu operațional și ca instrument esențial în conducerea operațiilor militare într-o eră dominată de confruntarea între *„sisteme de sisteme bazate pe informații".* În acest context, unul dintre cele mai importante progrese în domeniul *„informatizării"* îl reprezintă constituirea Forței de Sprijin Strategic a APL, structură dedicată coordonării tuturor aspectelor informaționale ale războiului, incluzând atacul și apărarea cibernetică, precum și războiul electronic. Acestor structuri statale li se pot alătura și alte forțe special antrenate pentru a duce acțiuni ofensive sau defensive în spațiul cibernetic, precum actori statali sponsorizați de stat, actori non-statali sau chiar patrioți, care acționează din propriile convingeri.

Pentru viitor, RPC își propune să dezvolte infrastructura digitală la nivel global, creând, astfel, dependențe economice și, implicit, politice pentru multe state. Această strategie consolidează rolul RPC ca actor mondial și îi oferă o influență considerabilă în procesele decizionale la nivel internațional, mai ales în legătură cu politicile sale privind Taiwanul. După cum a subliniat ambasadorul general al SUA pentru Spațiul Cibernetic și Politica Digitală în 2023, strategia RPC de a construi infrastructura globală a internetului – de la fibră optică și sateliți la centre de date și tehnologie wireless – arată că focalizarea doar pe securitatea datelor și a aplicațiilor ar însemna, în final, *„livrarea unor pachete foarte securizate și necorupte direct la Beijing, în cadrul unei arhitecturi fără încredere"* (Hamilton, 2024).

POLITICILE NATO ÎN SPAȚIUL CIBERNETIC

NATO a avut o evoluție semnificativă în ceea ce privește politica și viziunea sa în spațiul cibernetic. Analiza evoluției politicii NATO în domeniul cibernetic reflectă o adaptare continuă la amenințările din ce în ce mai complexe și diverse din mediul digital. Plecând de la Războiul Rece, unde puterea globală avea o componentă bicefală, ajungem la situația contemporană, unde este posibil ca acea *„capcană a lui Tucidice"* să fie mai valabilă ca niciodată. Pe măsură ce RPC, Federația Rusă sau orice altă țară dorește să devină din ce în ce mai influentă pe scena globală, există temeri că fricțiunile economice, cibernetice, militare sau geopolitice ar putea escalada într-un conflict major, deși există și posibilitatea evitării acestora prin diplomație și cooperare. Astfel, conceptul subliniază cât de riscant poate deveni

peisajul geopolitic atunci când o națiune în ascensiune economică, militară sau de altă natură provoacă o altă națiune, deja consacrată.

Fie că vorbim de RPC sau de NATO, acțiunile lor în spațiul cibernetic au o strânsă legătură cu istoria și cu regimul de conducere politică al acestora. Astfel, regimul autocratic de la Beijing încearcă să controleze și să cenzureze activitățile din spațiul cibernetic, pe când NATO militează pentru un spațiu cibernetic comun, deschis și sigur. Securitatea și apărarea cibernetică fac parte din misiunea fundamentală a NATO, cea de apărarea colectivă. Obiectivele principale ale sale în acest domeniu sunt de a-și proteja propriile rețele, de a opera în spațiul cibernetic, de a ajuta aliații să își consolideze reziliența în vederea protejării rețelelor naționale și de a oferi o platformă de consultare și de acțiune colectivă.

Direcția politicilor de securitate cibernetică a NATO este determinată de amenințarea crescândă a atacurilor cibernetice sponsorizate de stat. Ca răspuns, statele membre ale Organizației Atlanticului de Nord adoptă din ce în ce mai mult strategii de apărare cibernetică activă. Acestea combină detectarea atacurilor în timp real cu contramăsuri proactive, cu scopul de a reduce potențialele daune. Statele Unite și Regatul Unit conduc în ceea ce privește implementarea acestora, utilizând răspunsuri tehnice și politice, inclusiv hackback-uri, pentru a descuraja și a atribui amenințările cibernetice (Jun, 2023).

Apărarea cibernetică a apărut pe agenda NATO la Summitul de la Praga, din 2002, şi, ulterior, a fost confirmată ca prioritară în 2006, la Summitul de la Riga. Pentru prima dată a fost agreată o politică în acest sens, de către șefii de state şi de guverne, la Summitul de la București, în aprilie 2008. Evoluția rapidă, caracterul sofisticat și frecvența tot mai mare a amenințărilor și atacurilor cibernetice la adresa securității Alianței au reiterat apariția temei pe agenda de securitate a NATO. Conceptul Strategic adoptat la Summitul de la Lisabona, în anul 2010, recunoaște că atacurile din spațiul cibernetic pot afecta securitatea infrastructurilor critice naționale și pot pune în pericol *„prosperitatea, securitatea şi stabilitatea națională şi euroatlantică"* (NATO Strategic Concept, 2010), iar impactul lor ar putea fi la fel de dăunător precum un atac convențional. În consecință, la Lisabona s-au pus bazele dezvoltării de către Alianță a capacității de prevenire, detectare şi apărare împotriva acestor amenințări, dar și de redresare în urma apariției lor.

În 2014, la Summitul din Țara Galilor, nimeni nu a negat că operațiile din spațiul cibernetic ar putea avea un impact egal cu cel al atacurilor convenționale. Mai mult decât atât, s-a recunoscut, pentru prima dată, posibilitatea ca un membru să invoce Articolul 5 ca urmare a unui atac cibernetic de o magnitudine însemnată,

similar celor cu care s-a confruntat Estonia în 2007. Ca urmare a acestor atacuri cibernetice din Estonia, NATO a aprobat, în anul 2008, prima sa politică privind apărarea cibernetică și a înființat Centrul de Excelență pentru Apărare Cibernetică afiliat NATO (Cooperative Cyber Defence Centre of Excellence/CCDCOE), la Tallinn.

La conferința de securitate de la München, din 2011, NATO a adoptat o nouă politică de apărare cibernetică, care se concentrează pe prevenirea atacurilor cibernetice și construirea rezilienței. Crearea echipei de reacție rapidă a fost rezultatul revizuirii politicii de apărare cibernetică a Alianței, dar și implementarea unei capabilități de apărare cibernetică a propriilor rețele (Hasanov, Iskandarov, Sadiyev, 2019). Ca urmare a lecțiilor identificate și însușite din amenințările și atacurile cibernetice de până atunci, marile puteri și-au intensificat activitatea în mediul digital concomitent cu dezvoltarea de legi, strategii, politici și doctrine care reglementează activitatea.

Ca o consecință a activităților cibernetice de până atunci, în iulie 2016, în cadrul Summitului de la Varșovia, aliații au recunoscut spațiul cibernetic ca fiind un domeniu operațional în care NATO trebuie să se apere la fel de *„eficient ca în aer, pe uscat și pe mare”* (NATO, 2016). Aliații au convenit asupra unei viziuni și strategii militare pentru operațiile din spațiul cibernetic și s-au angajat să acționeze cu prioritate pentru consolidarea capacităților cibernetice naționale, asumându-și un angajament politic în acest sens *(Cyber Defence Pledge)*, pentru sporirea rezilienței rețelelor și infrastructurilor naționale, precum și pentru îmbunătățirea reacției de răspuns rapid și eficient la atacurile cibernetice. După cum era de așteptat, la Summitul NATO din 2018, de la Bruxelles, aliații au convenit să înființeze un *Centru de Operații în Spațiul Cibernetic (Cyber Operations Center/CYOC)*, ca parte a structurii de comandă consolidate a NATO. De asemenea, au consimțit faptul că NATO poate apela la capacitățile cibernetice naționale ale statelor membre pentru operațiile și misiunile Alianței. Un an mai târziu, în februarie 2019, aliații au aprobat un ghid NATO care stabilește o serie de instrumente (politice, diplomatice, militare) pentru a consolida capacitatea NATO de a răspunde la acțiunile cibernetice rău intenționate (NATO, 2024).

La Summitul NATO din 2023, organizat la Vilnius, aliații au adoptat un nou *Concept* destinat să îmbunătățească contribuția apărării cibernetice și de descurajare a Alianței. De asemenea, membrii Alianței au reafirmat și întărit angajamentul lor față de apărarea cibernetică, stabilind obiective mai ambițioase pentru consolidarea apărării cibernetice naționale, inclusiv a infrastructurilor critice. Conștientizând nevoia de asistență rapidă, NATO a inițiat *Capabilitatea Virtuală de Sprijin în caz*

de Incidente Cibernetice (Virtual Cyber Incident Support Capability) pentru a ajuta la eforturile naționale de atenuare a incidentelor cibernetice semnificative (NATO, 2023). Este interesant faptul că, în comunicatul precedat de summit, numele Republicii Populare Chineze apare de două ori. Interesele și politicile coercitive ale Republicii Populare Chineze sunt recunoscute ca reprezentând o provocare directă pentru interesele, securitatea și valorile internaționale. RPC își folosește o varietate de instrumente politice, economice și militare pentru a-și extinde influența globală și pentru a-și proiecta puterea. De asemenea, efectuează operații hibride și cibernetice nocive, folosește retorică agresivă și practică dezinformarea, vizând aliații și compromițând securitatea aliaților. RPC încearcă să domine sectoarele cheie tehnologice, industriale și infrastructura critică și să controleze materialele strategice și lanțurile de aprovizionare. Utilizează influența economică pentru a crea dependențe strategice și pentru a-și mări influența, străduindu-se să submineze ordinea internațională bazată pe norme, inclusiv în domeniile spațial, cibernetic și maritim (Ib.). De asemenea, tot în acel comunicat se mai prezintă faptul că instabilitatea din Africa și Orientul Mijlociu afectează în mod direct securitatea, atât a NATO, cât și a partenerilor. Alianța se confruntă cu amenințări cibernetice, spațiale, hibride și alte asimetrice, iar intențiile clare și politicile coercitive ale Guvernului de la Beijing, sfidează interesele și pun în pericol securitatea NATO (Ib.). Practic, din acest moment, Republica Populară Chineză este recunoscută oficial de către NATO ca fiind, dacă nu un adversar, cel puțin un competitor semnificativ în domeniul cibernetic.

La Summitul NATO din 2024, de la Washington, D.C., aliații au decis înființarea unui nou Centru Integrat de Apărare Cibernetică la SHAPE, pentru a îmbunătăți protecția rețelelor și implementarea cibernetică în diverse scenarii de pace, criză și conflict. NATO încurajează, de asemenea, o abordare unitară în dezvoltarea capabilităților de apărare cibernetică prin stabilirea de obiective specifice pentru țările aliate, sprijinindu-le să își consolideze apărarea națională cibernetică prin schimbul de informații și bune practici și prin organizarea de exerciții specializate. Această facilitate permite statelor membre să contribuie voluntar la întărirea capabilităților cibernetice ale altor aliați (NATO, 2024).

Pe parcursul ultimului deceniu, politicile cibernetice ale NATO au facilitat și dezvoltarea legăturilor cu instituțiile civile ale Uniunii Europene, consolidând, astfel, parteneriatele de colaborare civil-militare. Această dinamică se manifestă în contextul în care majoritatea statelor membre ale UE sunt, de asemenea, state membre ale NATO. Apărarea cibernetică este unul dintre domeniile de cooperare

consolidată între NATO și UE, ca parte a eforturilor tot mai coordonate ale celor două organizații de a contracara amenințările hibride. NATO și UE fac schimb de informații și de bune practici. De asemenea, cooperarea este consolidată în ceea ce privește formarea, cercetarea și exercițiile cu rezultate tangibile în combaterea amenințărilor cibernetice. Alianța Nord-Atlantică și Uniunea Europeană cooperează prin intermediul unui acord tehnic privind apărarea cibernetică, semnat în anul 2016. Având în vedere provocările comune, NATO și UE își consolidează cooperarea în domeniul apărării cibernetice, în special în ceea ce privește instruirea și răspunsurile la atacurile cibernetice.

AMENINȚĂRILE CIBERNETICE ALE REPUBLICII POPULARE CHINEZE ȘI IMPLICAȚII LA ADRESA SECURITĂȚII CIBERNETICE A NATO

Ascensiunea Republicii Populare Chineze a alimentat competiția dintre aceasta și SUA, în special în domeniul comerțului și al tehnologiei. Chiar SUA au recunoscut RPC drept *„singura țară care are atât voința, cât și capacitatea de a remodela ordinea regională și internațională”* (Zhang, 2024). Competiția dintre cele două superputeri are loc, de asemenea, într-un moment în care economiile bazate pe internet și elaborarea politicilor cibernetice gravitează din ce în ce mai mult în jurul celor trei modele principale stabilite de SUA, RPC și UE. Politicile chinezești de securitate cibernetică rămân în centrul dezbaterilor și cercetărilor la nivel mondial (Jiang, M. , 2023). Spațiul cibernetic este un mediu inerent nesigur, astfel încât amenințările cibernetice reprezentate de RPC la adresa securității NATO sunt multiple și complexe, având implicații semnificative asupra securității Alianței și a statelor membre.

Zilnic se raportează mii de amenințări cibernetice în întreaga lume, iar multe dintre ele sunt atribuite Republicii Populare Chineze. Un studiu recent a considerat RPC drept *„cea mai cuprinzătoare putere cibernetică”* după SUA, fapt datorat prioritizării educației în domeniul științei și tehnologiei informațiilor și formării specialiștilor pentru operațiile militare cibernetice (Hlavek, 2021). După cum era de așteptat, principala țară vizată de operațiile chinezești din spațiul cibernetic sunt SUA, cel mai puternic stat membru al NATO. De asemenea, și Washingtonul a identificat Beijingul ca fiind cea mai importantă amenințare de spionaj, cu peste 300 de miliarde de dolari pierderi anuale din furtul de proprietate intelectuală (Kobzova, 2023). În plus, alte state membre ale NATO, în special din Europa, au raportat atacuri provenite de la hackerii chinezi. Aceste atacuri s-au intensificat când o serie de state europene au interzis firmelor din RPC să participe la dezvoltarea

tehnologiei 5G din statele respective (Reuters, 2023). Companiile chinezești de IT, printre care și Huawei, beneficiază de un suport substanțial din partea guvernului, inclusiv subvenții și investiții în cercetare și dezvoltare, ceea ce le-a propulsat pe unele dintre acestea, în special Huawei, în fruntea industriei globale a tehnologiei 5G, alături de alte companii occidentale de renume. Introducerea tehnologiei 5G de către firmele chinezești pe piețele globale a întâlnit opoziția vehementă din partea unor state occidentale, ai căror lideri politici sunt preocupați de riscurile de securitate asociate cu tehnologia chineză și de potențialul ei de a fi folosită în scopuri de spionaj sau disruptive (The International Institute for Strategic Studies, 2021).

Mai mult decât atât, în iulie 2023, au fost identificate noi operații cibernetice în țări membre ale NATO precum Marea Britanie, Slovacia, Republica Cehă și Ungaria (Sharwood, 2023). Țintele frecvente au foste reprezentate de entitățile diplomatice, ministerele de externe, sectorul privat și diferite alte instituții. Cu câteva luni înainte, Agenția Uniunii Europene pentru Securitate Cibernetică/ENISA a emis un raport în care a expus numeroase cazuri de atacuri de spionaj cibernetic asupra statelor membre, inclusiv activități îndreptate împotriva unor companii germane, a unor ministere belgiene, organizații franceze, instituții ale UE și multe altele (ENISA, CERT-EU, 2023). Pe de altă parte, culegerea de date și alte informații despre cetățenii sau instituțiile statelor membre ale NATO prin intermediul diferitelor platforme media sporește și mai mult avantajul strategic al Beijingului în fața competitorilor săi. Împreună cu investițiile sale masive în tehnologiile emergente și în educarea specialiștilor, Beijingul și-a îmbunătățit tehnicile, tacticile și eficiența prin complexitatea operațiilor din mediul digital. Îmbinarea tuturor acestor elemente a consolidat poziția de lider a RPC, devenind una dintre cele mai importante provocări cu care se confruntă NATO (Kobzova, ib.).

Obiectivul general al amenințărilor vizate de RPC este de a câștiga avantaj pe plan politic, militar și economic în raport cu națiunile occidentale. Din punct de vedere al securității cibernetice, abordarea strategică a Beijingului se distinge de cea a altor actori semnificativi din acest domeniu, precum Federația Rusă, Coreea de Nord sau Iranul. Scopul nu e de a compromite infrastructura critică, ci, mai degrabă, de spionaj cibernetic. De-a lungul timpului, Beijingul a câștigat notorietate pentru activitățile sale de spionaj cibernetic susținute atât în sectorul industrial, cât și în cel militar. Totuși, merită menționat faptul că, în anumite ocazii, hackerii chinezi au fost implicați și în atacuri care au vizat perturbarea infrastructurii critice (Ib.).

Un alt aspect al confruntării dintre RPC și SUA o constituie zona de influență geostrategică Asia-Pacific, unde cele două mari puteri au interese. Una dintre cele mai recente și îngrijorătoare campanii cibernetice ale RPC a vizat insula americană Guam (Sanger, 2023). Operația cibernetică din Guam a evidențiat rolul strategic al acestui teritoriu, având în vedere poziționarea sa geografică apropiată de Taiwan și facilitățile militare importante pe care le deține, esențiale pentru capacitatea de răspuns a Statelor Unite în eventualitatea escaladării conflictului din Marea Chinei de Sud. Aceste atacuri cibernetice, care au vizat infrastructuri critice precum bazele militare și sistemele de transport și telecomunicații, indică o deviere semnificativă de la metodele convenționale de spionaj cibernetic, sugerând un obiectiv dual al acestora: recunoașterea și potențiala pregătire pentru acțiuni disruptive. În susținerea acestei informații, un raport publicat de Noua Zeelandă și Canada a indicat faptul că malware-ul chinezesc nu a fost destinat exclusiv spionajului cibernetic (Kobzova, ib.).

În *Global Threat Report* din 2022, compania americană de securitate cibernetică *Crowd Strike* a clasificat RPC ca fiind lider mondial în exploatarea vulnerabilităților cibernetice. Raportul evidențiază competențele avansate de exploatare deținute de comunitatea de hackeri chinezi, subliniind, astfel, capacitatea semnificativă de dezvoltare tehnică a cesteia (U.S.-China Economic and Security Review Commission, 2022). În conformitate cu alte rapoarte publice, de-a lungul ultimelor două decenii, RPC a fost continuu implicată în operații cibernetice ofensive. Odată cu extinderea ambițiilor sale economice și politice, influența sa în spațiul cibernetic a crescut semnificativ. Acest lucru este reflectat de numărul tot mai mare de actori non-statali sponsorizați de stat, care dezvoltă și implementează capacități cibernetice ofensive în sprijinul obiectivelor naționale, variind de la securitatea economică până la cea națională(Handler, 2023). Ca un răspuns la toate activitățile din spațiul cibernetic care au implicat NATO sau membri ai acesteia, șefii de state și de guverne au luat unele măsuri, fie reactive sau proactive, în funcție de situație.

Odată cu proliferarea și sofisticarea amenințărilor – inclusiv terorismul, atacurile cibernetice, tehnologiile disruptive, schimbările climatice și provocările din partea Rusiei și RPC la adresa ordinii internaționale –, NATO a adoptat *Inițiativa NATO 2030*. Acest document vizează consolidarea cooperării transatlantice și abordarea proactivă a problemelor de securitate legate de tehnologiile emergente și disruptive, răspunzând ambițiilor RPC de a domina sectorul inteligenței artificiale. Prin această inițiativă, NATO se angajează să investească în extinderea și aprofundarea parteneriatelor strategice care reflectă valorile și interesele comune, consolidând,

astfel, cooperarea transatlantică. De asemenea, activitățile RPC în spațiul cibernetic sunt considerate amenințări care necesită o adaptare strategică profundă și rapidă din partea NATO pentru a rămâne eficient și relevant în protejarea securității și prosperității membrilor săi (NATO, 2021).

Drept urmare, pentru a gestiona eficient incidentele cibernetice, NATO se angajează într-o pregătire continuă și coordonată. În acest sens, reprezentanții statelor membre au convenit asupra înființării unor instituții dedicate, capabile să prevină, să răspundă prompt și să remedieze rapid problemele de securitate în rețelele Alianței. Aceste structuri sunt esențiale pentru consolidarea rezilienței NATO împotriva amenințărilor cibernetice și pentru menținerea stabilității operaționale în fața provocărilor moderne.

Din punct de vedere operațional, Alianța Nord-Atlantică a creat un Centru de Operații în Spațiul Cibernetic în cadrul Comandamentului Aliat pentru Operații (ACO) din Mons, Belgia, în anul 2019. Scopul principal al acestui centru este de a monitoriza spațiului cibernetic și a coordona și sincroniza operațiile din acest domeniu cu cele din domeniile terestru, maritim și aerian (Brzozowski, 2018). Acest centru este esențial pentru securitatea cibernetică a Alianței, deoarece poate reprezenta un factor de descurajare și îi permite NATO să răspundă rapid și eficient la potențialele atacuri cibernetice. De asemenea, centrul îmbunătățește colaborarea între statele membre și poate constitui baza pentru un Comandament Cibernetic NATO esențial în fața amenințărilor cibernetice în continuă evoluție.

Din perspectiva tehnică, Agenția NATO pentru Comunicații și Informatică (NCIA) interacționează cu Centrul NATO pentru Securitate Cibernetică (NCSC) și cu Capabilitatea NATO de Răspuns la Incidente Informatice (NCIRC), fiind responsabilă de dezvoltarea, gestionarea și securizarea infrastructurii cibernetice a Alianței. Pe de altă parte, NCIRC monitorizează în permanență rețelele, fiind prima structură care răspunde în cazul unor atacuri, întocmește rapoarte privind cazuri similare și oferă sprijin statelor membre. În plus, NCIRC, prin intermediul unui centru de coordonare specific, permite statelor membre să facă schimb de informații și tehnici privind amenințările cibernetice, inclusiv unii indicatori care pot oferi indicii cu privire la natura atacurilor produse. Aceste structuri ale NATO au contracte cu companii din domeniul apărării, lideri pe piața IT, privind serviciile de protecție informatică pentru Alianță. Mai mult decât atât, echipele NATO de reacție rapidă în domeniul cibernetic sunt disponibile pentru a fi utilizate prompt în sprijinul aliaților care suferă atacuri cibernetice (Marrone, Sabatino, 2021). Acest tip de parteneriat

civil-militar întărește cooperarea și reziliența în ceea ce privește securitatea și apărarea în domeniul cibernetic.

Este general cunoscut faptul că provocările în spațiul cibernetic sunt considerabil diferite de cele din alte domenii operaționale, deoarece este un domeniu artificial, creat de om și controlat aproape în totalitate de acesta. În acest context, resursa umană este esențială. Drept urmare, pregătirea adecvată a personalului devine crucială pentru prevenirea incidentelor cibernetice sau pentru gestionarea eficientă a celor existente. NATO investește în mod strategic în formarea specialiștilor săi, organizând cursuri intensive la diverse instituții academice afiliate Alianței.

Capacitățile cibernetice ale RPC reprezintă o îngrijorare în cadrul Alianței Nord-Atlantice, de aceea au fost luate numeroase măsuri în contrapartidă. În spațiul cibernetic, NATO ar trebui să își asume rolul de lider în cadrul comunității internaționale, în ceea ce privește legislația și reglementările juridice. În consecință, Alianța a înființat Centrul de Excelență pentru Cooperare în domeniul Apărării Cibernetice (CCDCOE) la Tallinn, instituție care are scopul de a întări capacitățile de apărare cibernetică. Acest centru servește drept hub principal pentru cercetare și gândire strategică în domeniul cibernetic, facilitând nu doar cercetarea avansată, ci și dezvoltarea de strategii inovative de apărare cibernetică. De asemenea, pune accent pe dezvoltarea doctrinelor, instruire și educație, pentru a sprijini interoperabilitatea și schimbul de bune practici între membrii și partenerii NATO. În cadrul acestui centru s-a elaborat un ghid cuprinzător privind normele și legile aplicabile în domeniul războiului cibernetic, numit *Manualul de la Tallinn* (Pfannenstiel, Cox, 2024). Acesta este un document academic elaborat pentru a oferi o interpretare detaliată a modului în care legile internaționale existente se aplică conflictelor cibernetice. Acest tratat ar consolida securitatea globală și ar permite NATO să se apere mai eficient împotriva amenințărilor chinezești. Totodată, specialiștii NATO beneficiază de oportunități numeroase de antrenament prin participarea la exerciții și activități comune, organizate de Alianță sau în colaborare cu alți parteneri. Spre exemplu, în anul 2023, peste 3.000 de participanți din 38 de țări – inclusiv aliați și parteneri NATO – au participat la exercițiul anual *„Locked Shields”,* găzduit de CCDCOE. Acesta este cel mai mare exercițiu de apărare cibernetică din lume și a implicat protejarea sistemelor informatice de atacuri în timp real și simularea deciziilor tactice și strategice în situații critice (NATO, 2023).

Astfel de exerciții sunt fundamentale pentru consolidarea cooperării și pentru facilitarea schimbului de bune practici, jucând un rol esențial în consolidarea

legăturilor dintre națiunile membre. Prin aceste exerciții se creează oportunități valoroase pentru aliați de a testa și îmbunătăți procedurile comune în situații simulate, crescând, astfel, eficacitatea răspunsurilor în caz de criză reală. Mai mult, aceste activități oferă o perspectivă nouă asupra importanței colaborării civile-militare. Prin implicarea entităților civile, inclusiv universități și instituții de cercetare din sectorul privat, exercițiile contribuie nu doar la îmbunătățirea capabilităților de apărare cibernetică, ci și la consolidarea sinergiilor dintre resursele civile și cele militare, un factor crucial în adaptarea la noile provocări tehnologice și în gestionarea amenințărilor cibernetice complexe.

Într-un context global tot mai dependent de tehnologie, astfel de inițiative sunt vitale pentru menținerea unui avantaj strategic în spațiul cibernetic. Ele nu doar că întăresc capacitățile individuale ale fiecărui stat membru, dar asigură și o bază solidă pentru o apărare colectivă eficientă. De asemenea, exercițiile, alături de alte inițiative similare, au un rol foarte important în descurajarea adversarilor, permițând Alianței să răspundă prompt și coeziv la amenințările emergente și să protejeze infrastructurile critice din statele membre. Aceste activități consolidează capacitatea NATO de a anticipa și contracara eficient potențialele atacuri, asigurând, astfel, securitatea și stabilitatea regiunii.

O altă măsură pe care ar trebui să o aplice NATO ar fi aceea de a investi mai mult în echipamente, în dezvoltarea tehnologiilor emergente, în specializarea personalului și dezvoltarea igienei cibernetice în rândul populației, astfel încât să contracareze efectul disruptiv al acțiunilor ofensive care vizează securitatea Alianței. De asemenea, NATO poate rămâne competitivă în domeniul apărării și securității cibernetice doar printr-o cooperare strânsă cu instituțiile civile, academice și private, iar prin această sinergie civil-militară, Alianța va putea să aibă un răspuns comprehensiv în cazul amenințărilor cibernetice. Mai mult decât atât, îmbunătățirea schimbului de informații și a practicilor de colaborare între statele membre, prin utilizarea unor platforme comune pentru partajarea datelor despre amenințări și vulnerabilități în timp real, va fi extrem de benefică.

Nu în ultimul rând, prin diplomație cibernetică se pot stabili norme și reguli internaționale privind comportamentul în spațiul cibernetic, încercând să se construiască un acord global privind interzicerea unor practici disruptive care ar putea vătăma, fără remediere, date, rețele și infrastructuri critice.

CONCLUZII

Acest studiu nu se dorește a fi o cercetare exhaustivă, drept pentru care abordarea sa se limitează la aspecte specifice ale securității cibernetice, fără a explora în totalitate toate dimensiunile și plurivalențele geopolitice asociate. Aceasta reprezintă o delimitare intenționată a scopului și amplitudinii analizei, concentrându-se pe contribuții punctuale ale politicilor și a literaturii de specialitate existente.

Limitările din această cercetare au constat din alegerea pentru studiu doar a unei singure alianțe, ceea ce a permis o focalizare detaliată, dar a restricționat, de asemenea, posibilitatea de a generaliza constatările la alte state sau alianțe. În plus, materialele din surse deschise pe această temă sunt adesea contradictorii, sumare și neclare. Această decizie metodologică a fost determinată de necesitatea unei analize aprofundate, care, în ciuda specificității sale, oferă o bază solidă pentru extrapolări ulterioare și cercetări comparative în domeniul securității cibernetice. Drept urmare, direcțiile de cercetare viitoare ar putea include analiza activităților cibernetice și impactul acestora asupra securității cibernetice atât la nivelul Uniunii Europene, cât și în context internațional. Prin urmare, pentru o înțelegere adecvată, securitatea cibernetică necesită o perspectivă holistică care să integreze și să analizeze multiplele sale dimensiuni și interacțiunile dintre acestea.

Răspunsul la întrebarea de cercetare nu este simplu. Securitatea cibernetică în cadrul unei alianțe trebuie evaluată dintr-o perspectivă multistratificată și completă. Până în prezent, Republica Populară Chineză nu a pus la grea încercare Alianța Nord-Atlantică; totuși, ambițiile sale de a domina spațiul cibernetic se conturează ca provocări iminente pentru NATO. În vederea unei mai bune gestionări a incidentelor cibernetice, au fost propuse diverse măsuri.

În cele din urmă, NATO trebuie să adopte o abordare comprehensivă în fața amenințărilor cibernetice ale RPC, investind în tehnologiile emergente, în consolidarea cooperării cu partenerii civili și militari și în educația specialiștilor din domeniul cibernetic. Totodată, prin exerciții comune și diplomație cibernetică, NATO poate contribui la dezvoltarea unui cadru internațional care să promoveze un comportament responsabil în spațiul cibernetic. Răspunsul Alianței trebuie să fie unul bazat pe prevenție, descurajare și cooperare, pentru a păstra stabilitatea și securitatea într-un domeniu tot mai contestat.

BIBLIOGRAFIE:

1. Austin, G. (2018). *Cybersecurity in China The Next Wave.* Canberra: Springer.
2. Brzozowski, A. (17 octombrie 2018). *NATO sees new cyber command centre by 2023 as Europe readies for cyber threats*.
3. Burke, E.J., Gunness, K., Cooper III, C.A., Coza, M. (2020). *People's Liberation Army Operational Concepts.* Santa Monica: RAND .
4. Chafetz, G. (31 iulie 2023). *How China's Political System Discourages Innovation and Encourages IP Theft.* SUA.
5. Denning, D.E. (2001). *Chapter Eight – Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. În J. Arquilla, D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239-288). RAND Corporation.
6. Diotte, P. (2020). *The Big Four and Cyber Espionage: How China, Russia, Iran and North Korea Spy Online*. În *Canadian Military Journal*, pp. 32-42.
7. ENISA, CERT-EU (2023). *JP-23-01 – Sustained activity by specific .*
8. Ford, C.A. (11 septembrie2019). *U.S. Department of States*, https://2017-2021.state.gov/: https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/, accesat la 22 iulie 2024
9. Grauman, B. (2012). *Cyber-Security: The Vexed Question of Global Rules.*
10. Hamilton, B.A. (2020). *Same Cloak, More Dagger: Decoding How the People's Republic of China Uses Cyberattacks,* https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html#report, accesat la 22 iulie 2024.
11. Hamilton, B.A. (2024). *How to succeed at annexation without really fighting – The PRC's Taiwan Cyber Strategy Explained.*
12. Handler, S. (31 ianuarie 2023). *The 5×5 – China's cyber operations*, https://www.atlanticcouncil.org/: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/, accesat la 22 iulie 2024.
13. Hasanov, A.H., Iskandarov, K.I., Sadiyev, S.S. (2019). The Evolution of Nato's Cyber Security Policy and Future Prospects. În *Journal of Defense Resources Management,* vol. 10, nr. 1(18), pp. 94-106.
14. Hlavek, A. (2021). *China cyber attacks: the current threat landscape.* Ironnet.
15. Hwang, J.-J. (2023). *Reframing China's Territory and Sovereignty in Cyberspace: Exploring Conceptual Territorialization and Claims of Cyber Sovereignty*. În *Issues & Studies A Social Science Quarterly on China, Taiwan and East Asian Affairs,* vol. 59, nr. 4, 21.
16. Jiang, M. (2020). *Cybersecurity policies in China*. În L. Belli, *CyberBRICS: Cybersecurity Regulations in BRICS Countries* (pp. 95-212). Berlin: Springer.
17. Jiang, M. (2023). *Chinese Cybersecurity Policies in the Age of Cyber Sovereignty*. În M. Timoteo, B. Verri, R. Nanni, *Quo Vadis, Sovereignty? New Conceptual and Regulatory Boundaries in the Age of Digital China* (pp. 77-90). Springer Nature Switzerland AG.
18. Jiang, T. (2019). *From Offensive Dominance to Detterrence: China's Evolving Strategic Thinking on Cyberwar*. În *Chinese Journal of International Review,* vol. 1, nr. 2, pp. 195-218, www.worldscientific.com., accesat la 17 iulie 2024.

19. Jiang, T. (2022). *The Shift of China's Strategic Thinking on Cyberwarfare Since the 1990s*. În *Journal of Chinese Political Science*, pp. 127-149.
20. Jinghua, L. (22 martie 2019), https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/, accesat la 29 iunie 2024.
21. Jun, O. (2023). *Direction of Japan's New Cybersecurity Policy*. În *Asia-Pacific Review*, pp. 63-78.
22. Kobzova, L. (2023). *China's Cyber Threat: Implications for NATO and Potential Remedies.* Adapt Institute.
23. Marrone, A., Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models.* Instituto Affari Internazionali.
24. NATO Strategic Concept (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Lisbon: NATO.
25. NATO/North Atlantic Threaty Organization (2016). Warsaw Summit Communiqué. Warsaw .
26. NATO/North Atlantic Treaty Organization (2021). *NATO 2030.*
27. NATO/North Atlantic Treaty Organization (14 septembrie 2023). *North Atlantic Treaty Organization*, https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 28 iulie 2024.
28. NATO/North Atlantic Treaty Organization (2023). Vilnius Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_217320.htm, accesat la 27 iunie 2024.
29. NATO/North Atlantic Treaty Organization (30 iulie 2024). *Cyber defence*, North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 29 iunie 2024.
30. Pfannenstiel, M., Cox, D. (2024). *NATO's Cyber Era (1999–2024) Implications for Multidomain Operations*. *Military Review Online Exclusive*.
31. Reuters (29 septembrie 2023). *European countries who put curbs on Huawei 5G equipment*, https://www.reuters.com/: https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/, accesat la 29 iunie 2024.
32. Sanger, D.E. (24 mai 2023), în Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html, accesat la 29 iunie 2024.
33. Sharwood, S. (4 iulie 2023). *Undiplomatic Chinese threat actors attack embassies.*
34. Soesanto, S. (4 iulie 2022). *Cyber Detterence Revisited*. Alabama: Air University Press.
35. The International Institute for Strategic Studies (2021). *Cyber Capabilities and National Power: A Net Assessment.*
36. The State Council Information Office of the People's Republic of China. (iulie 2019). *China's National Defense in the New Era*. Beijing, China: Foreign Languages Press Co. Ltd.
37. The White House (mai 2011). International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World. Washington.

38. Triolo, P., Sacks, S. (26 septembrie 2017). *Center for Strategic and International Studies*, https://www.csis.org/analysis/shrinking-anonymity-chinese-cyberspace: https://www.csis.org, accesat la 29 iunie 2024.
39. United Nations General Assembly (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.*
40. U.S.-China Economic and Security Review Commission (2022), https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf, accesat la 29 iunie 2024.
41. Zhang, H. (12 iulie 2024). *What is the intention of NATO, the „war maker", to „directly warn" China?* China.