Reconfigurarea surselor de putere în secolul XXI: cyber intelligence. Studiu de caz: Federația Rusă

Rezumatul tezei

Coordonator: Prof. univ. dr. amb. George-Cristian MAIOR

Doctorand: Dragoș VETRESCU

Introducere și obiectivul cercetării: Această teză de doctorat, intitulată *„Revisioning the Sources of Power in the 21st Century: Cyber Intelligence. Case study: Russian Federation” / „Reconfigurarea surselor de putere în secolul XXI: cyber intelligence. Studiu de caz: Federația Rusă”*, examinează modul în care intelligence-ul din spațiul cibernetic (cyber intelligence) acționează ca un multiplicator de forță în sfera politicii internaționale de putere. Cercetarea abordează o problemă actuală în relațiile internaționale: în ce măsură capabilitățile cibernetice, în special cele legate de culegerea de informații și operațiuni cibernetice ofensive, pot spori puterea și influența unui stat pe scena globală. Obiectivul principal al studiului este de a determina gradul în care informațiile cibernetice pot amplifica puterea unui stat, analizând acest fenomen prin prisma cazului Federației Ruse, de importanță deosebită în actualul context internațional, și în special pentru țara noastră. Prin focalizarea asupra modului în care Rusia utilizează astfel de instrumente cibernetice, teza își propune să evidențieze dinamica modernă a puterii statale și să acopere o lacună în teoria relațiilor internaționale referitoare la impactul domeniului cibernetic asupra structurilor tradiționale de putere.

Cadru teoretic: Studiul se fundamentează pe teoriile relațiilor internaționale și ale studiilor de securitate, în special pe conceptele de politică de putere (realpolitik) și de război hibrid, pe care le completează interdisciplinar cu concepte din sfera studiilor de intelligence. Teza conceptualizează cyber intelligence-ul ca un element emergent al puterii statale, capabil să potențeze instrumentele diplomatice, militare și informaționale tradiționale. Noțiunea de „multiplicator de forță” este utilizată în sens strategic, referindu-se la un factor care crește semnificativ eficacitatea capacităților existente ale unui stat. În acest context, lucrarea pornește de la ideea că operațiunile de intelligence în spațiul cibernetic — care includ operațiuni de spionaj cibernetic, război informațional și alte acțiuni cibernetice disruptive sau distructive — pot multiplica efectul acțiunilor unui stat fără a necesita recursul la forța militară convențională de mare anvergură. Această bază teoretică subliniază importanța abordării operațiunilor cibernetice nu doar ca probleme tehnice, ci ca instrumente strategice în competiția de putere dintre state.

Metodologie de cercetare: Teza utilizează o metodologie calitativă, de tip studiu de caz comparativ, urmând abordarea lui Stephen Van Evera pentru analiza structurată a ipotezelor. Printr-o comparație focalizată și structurată, sunt examinate în mod sistematic multiple instanțe (studii de caz) ale operațiunilor cibernetice desfășurate de Rusia. Această metodă presupune analizarea fiecărui caz selectat pe baza aceluiași set de întrebări și criterii, permițând o comparație coerentă între diferite evenimente. În fiecare caz sunt luați în considerare factori precum contextul geopolitic, obiectivele operațiunii cibernetice, tacticile și tehnicile utilizate, precum și rezultatele sau impactul asupra dinamicii puterii pe plan internațional. Urmând liniile directoare ale lui Van Evera, cercetarea verifică ipotezele propuse în raport cu evidențele empirice din fiecare caz, asigurând că concluziile sunt formulate prin inferență logică și *process tracing* (urmărirea proceselor cauzale). Sursele de date includ rapoarte de informații disponibile public (open-source), documente guvernamentale, analize de securitate cibernetică și studii academice, toate susținând o examinare temeinică a modului în care activitățile cibernetice de informații orchestrate de Rusia au fost implementate și cu ce efect.

Ipoteze de lucru: Obiectivul general al cercetării este de a examina modalitatea în care capabilitățile din sfera cyber intelligence influențează dinamicile puterii în sistemul internațional, utilizând Rusia ca studiu de caz. Așadar întrebarea centrală de cercetare este: Care este rolul cyber intelligence-ului în competiția internațională de putere în domeniul cibernetic?

Din această întrebare cadru derivă următoarele întrebări secundare la care teza își propună să răspundă:

1. Ce este cyber intelligence, și cum funcționează ca instrrument al puterii de stat?
2. Cum folosesc statele cyber intelligence pentru a-și amplifica influența geopolitică și a contracara adversari mai puternici?
3. În ce manieră utilizează Federația Rusă operațiuni din sfera cyber intelligence pentru a-și avansa obiectivele strategice, și care este impactul asupra dinamicii de putere la nivel global?
4. Cum ar putea tehnologiile emergente (precum inteligența artificială și computerele cuantice) să determine viitorul cyber intelligence în competiția globală pentru putere?

În acest scop analiza este ghidată de câteva ipoteze fundamentale formulate pe baza literaturii de specialitate și a cadrului teoretic:

1. **Statele cu capabilități avansate de cyber intelligence pot să își amplifice semnificativ puterea în sistemul internațional**. Această ipoteză postulează că statele cu capabilități cibernetice avansate (precum spionaj cibernetic, atacuri cibernetice strategice și operațiuni de influență online) pot atinge obiective de politică externă care depășesc, ca anvergură, ceea ce ar permite puterea lor militară sau economică tradițională. Cu alte cuvinte,

operațiunile cibernetice eficiente pot amplifica influența și eficacitatea unui stat în arena politicii internaționale.

2. **Utilizarea operațiunilor de intelligence în spațiul cibernetic de către Federația Rusă acționează ca un multiplicator de forță, permițându-i să conteste sau să perturbe ierarhia puterii dominată de state tradițional mai puternice.** Această ipoteză susține că operațiunile extinse ale Rusiei în spionajul cibernetic și operațiuni bazate pe intelligence (variabila independentă) au crescut în mod măsurabil influența geopolitică și puterea sa de negociere (variabila dependentă), permițându-i să joace un rol disproporționat pe scena internațională. Se sugerează astfel o legătură cauzală, prin care operațiunile cibernetice ale Rusiei contribuie la modificarea dinamicii puterii în domenii în care, în lipsa acestor capabilități, influența Rusiei ar fi mai limitată. Această ipoteză va fi testată prin studii de caz ale succeselor cyber intelligence ale Rusiei (precum atacuri cibernetice sau campanii strategice de influență) și ale consecințelor acestora asupra poziției Rusiei raportat la rivalii săi geopolitici.

3. **Cyber intelligence reprezintă un instrument asimetric capabil să contrabalanseze asimetria convențională a puterii între state.** Această ipoteză generală sugerează că până și statele cu economii sau forțe militare mai slabe pot descuraja, constrânge sau obține concesii de la adversari mai puternici dacă posedă capabilități superioare în domeniul informațiilor cibernetice. În termeni formali: atunci când un stat mai slab (în metrici tradiționale) folosește eficient operațiuni de informații cibernetice (variabila independentă), acesta poate atenua sau neutraliza parțial avantajele unui stat mai puternic (variabila dependentă: reducerea decalajului de influență sau a capacității de impunere a costurilor). Aceasta va fi analizată prin studierea scenariilor în care operațiunile cibernetice desfășurate de un actor relativ mai slab (de exemplu, acțiuni cibernetice ale Rusiei împotriva țărilor NATO) au produs efecte disproporționate față de puterea globală a acelui actor.
4. **Integrarea tehnologiilor emergente precum inteligența artificială în capabilitățile de cyber intelligence va amplifica și mai mult impactul acestora asupra distribuției internaționale a puterii**. Această ipoteză prospectivă propune că, pe măsură ce statele vor integra inteligența artificială și învățarea automată în activitățile de informații în spațiul cibernetic (variabila independentă), eficacitatea și valoarea strategică a acestor operațiuni vor crește (variabila dependentă), ducând potențial la noi modificări în echilibrul puterii. Se anticipează că primii adoptatori ai inteligenței artificiale în domeniul informațiilor cibernetice ar putea obține un avantaj semnificativ, extinzând decalajul între statele cu capabilități cibernetice și cele care rămân în urmă. Dovezile pentru această ipoteză vor fi mai degrabă exploratorii, bazate pe tendințele actuale ale aplicațiilor inteligenței artificiale în informații (precum automatizarea analizei amenințărilor sau strategii îmbunătățite de atac cibernetic) și analizate în capitolul 6 pentru a proiecta implicațiile acestora asupra competiției pentru putere.

Aceste ipoteze fundamentale constituie cadrul de analiză pentru evaluarea comportamentului Rusiei și a efectelor campaniilor sale cibernetice, în așteptarea ca dovezile empirice să confirme (sau să nuanțeze) ideea că cyber intelligence reprezintă un veritabil multiplicator de forță în lumea contemporană.

Studiu de caz – Operațiunile cibernetice ale Rusiei: Cu focalizare pe cazul Rusiei, teza realizează o analiză detaliată a câtorva operațiuni cibernetice de referință atribuite actorilor statali ruși sau entităților afiliate statului. Fiecare studiu de caz examinează motivele, modul de execuție și consecințele respectivei operațiuni, ilustrând felul în care cyber intelligence a fost utilizat ca instrument de politică externă. Exemple notabile includ:

- **Amestecul în alegerile prezidențiale din SUA din 2016:** Teza examinează ingerința cibernetică a Rusiei în alegerile prezidențiale americane din 2016. Această operațiune a implicat spionaj cibernetic (intruziunea în sistemele de e-mail ale organizațiilor și ale personalităților politice) și război informațional (diseminarea informațiilor sustrase și amplificarea dezinformării prin intermediul rețelelor sociale). Studiul de caz evidențiază modul în care această campanie cibernetică a urmărit să submineze procesele democratice și să influențeze rezultatele politice într-o țară de prim rang pe scena globală. Constatările arată că, deși este dificil de măsurat impactul exact asupra rezultatului scrutinului, operațiunea a reușit să semene discordie și să alimenteze îndoieli privind integritatea sistemului electoral american. Din punct de vedere strategic, acest caz demonstrează capacitatea Rusiei de a-și proiecta puterea și influența în interiorul unui stat advers fără a recurge la o confruntare militară directă, aliniindu-se conceptului de informații cibernetice ca multiplicator de forță în atingerea obiectivelor sale de politică externă.
- **Atacurile cibernetice împotriva Ucrainei:** Un alt set important de exemple provine din conflictul în desfășurare dintre Rusia și Ucraina. Teza detaliază operațiuni precum atacurile cibernetice asupra rețelei electrice ucrainene din decembrie 2015 și decembrie 2016, care au provocat întreruperi temporare de electricitate pentru sute de mii de civili. Aceste atacuri fără precedent asupra infrastructurii critice au demonstrat cum mijloacele cibernetice pot completa agresiunea militară convențională (în contextul conflictului extins dintre Rusia și Ucraina) prin semănarea haosului și evidențierea vulnerabilităților adversarului. În plus, este analizat atacul informatic de tip malware NotPetya din 2017 care, țintind inițial instituții din Ucraina (de exemplu, prin compromiterea unui software de contabilitate pe scară largă în această țară), s-a transformat într-un incident cibernetic global ce a cauzat pagube de ordinul miliardelor de dolari la nivel mondial. Deși impactul nediscriminatoriu al lui NotPetya a depășit cu mult ținta inițială, acest eveniment a subliniat disponibilitatea Rusiei de a utiliza arme cibernetice extrem de agresive pentru a destabiliza un adversar. Prin aceste cazuri, cercetarea arată că operațiunile cibernetice ale Rusiei împotriva Ucrainei au servit multiple scopuri strategice: culegerea de informații, slăbirea funcțiilor economice și guvernamentale ale adversarului, descurajarea sprijinului occidental pentru Ucraina și transmiterea unui mesaj privind capabilitățile Rusiei către întreaga lume.

- **Alte operațiuni și tactici hibride:** Teza face referire și la alte operațiuni din sfera cibernetică și informațională, precum atacurile din 2007 împotriva Estoniei (unul dintre primele cazuri în care un stat a fost ținta unor atacuri masive de tip *denial-of-service* ca reacție la o dispută politică cu Rusia) și diverse campanii de dezinformare în Europa. Deși aceste exemple nu sunt analizate la fel de detaliat ca studiile de caz principale, ele oferă un context suplimentar privind evoluția strategiei cibernetice a Rusiei. Per ansamblu, se conturează un tipar conform căruia agențiile ruse de informații (precum GRU și FSB) au dezvoltat un arsenal cibernetic versatil — de la spionaj pur (infiltrarea și exfiltrarea de date confidențiale din rețele guvernamentale sau ale organizațiilor străine) până la operațiuni psihologice (răspândirea de propagandă sau narațiuni false în mediul online) — pe care îl utilizează într-o manieră coordonată pentru a-și promova interesele naționale.

Constatări cheie: Analiza studiului de caz dedicat Rusiei oferă dovezi solide că cyber intelligence a funcționat ca un multiplicator de forță pentru puterea Moscovei în politica internațională:

- **Influență amplificată și impact asimetric:** Operațiunile cibernetice ale Rusiei i-au permis Moscovei să acționeze dincolo de ponderea conferită de puterea sa convențională. De exemplu, prin amestecul în politica internă a Statelor Unite și a unor țări europene, Rusia a reușit să exercite o influență care depășește de obicei ceea ce ar fi posibil prin mijloacele sale convenționale (economice sau diplomatice). Capacitatea de a interveni de la distanță în procese politice sau în infrastructuri critice ale altor state oferă Rusiei un instrument asimetric — unul care poate complica procesul decizional al adversarilor și le poate impune costuri fără a implica o confruntare militară directă.
- **Integrare strategică (război hibrid):** Rezultatele indică faptul că informațiile cibernetice sunt integrate ferm în strategia mai amplă de „război hibrid" a Rusiei — un amestec de amenințări militare, operațiuni acoperite și război informațional. Tacticile cibernetice au fost utilizate în paralel cu cele convenționale (așa cum s-a observat în Ucraina) pentru a maximiza efectul. Această integrare acționează ca un multiplicator de forță prin potențarea operațiunilor tradiționale; de pildă, paralizarea comunicațiilor sau a alimentării cu energie ale adversarului poate pregăti terenul pentru operațiuni terestre mai eficiente sau, alternativ, hărțuirea și sabotajul cibernetic pot fi folosite acolo unde o acțiune militară directă nu este fezabilă.
- **Limitări și contramăsuri:** Cercetarea recunoaște, de asemenea, că, deși informațiile cibernetice oferă noi oportunități de exercitare a puterii, ele prezintă și limite. Nicio operațiune cibernetică nu a generat de una singură schimbări strategice decisive: de pildă, atacurile cibernetice nu au câștigat războaie în mod independent, iar țintele au devenit tot mai reziliente. Cazul atacurilor asupra rețelei electrice a Ucrainei arată că, deși disruptive, acele intruziuni nu au afectat determinarea Ucrainei și nici capacitatea sa de a riposta. Mai mult, operațiunile cibernetice agresive atrag adesea reacții internaționale adverse, sancțiuni și îmbunătățiri ale apărării cibernetice în statele vizate. Analiza constată că caracterul

iterativ al conflictelor cibernetice — acțiune și contraacțiune — implică faptul că efectul de multiplicare al forței se poate diminua în timp, pe măsură ce oponenții se adaptează. Cu toate acestea, în perioada studiată, Rusia a obținut avantaje considerabile pe termen scurt, profitând de surpriză și de secretul inerent operațiunilor cibernetice.

Contribuții originale ale cercetării: Prezenta lucrare aduce câteva contribuții importante atât literaturii de specialitate, cât și sferei practice a relațiilor internaționale în era digitală:

- **Cadru conceptual:** Teza elaborează un cadru conceptual pentru examinarea cyber intelligence prin lentila politicii de putere, tratând capabilitățile cibernetice ca variabile strategice ale puterii statului, alături de elemente tradiționale precum forța militară și pârghiile economice. În acest mod, lucrarea face legătura între domeniul securității cibernetice și teoria relațiilor internaționale, oferind o modalitate de a analiza operațiunile cibernetice în termeni de proiecție a puterii și echilibru al puterii.
- **Analiza empirică a cazului rus:** Cercetarea furnizează a analiză cuprinzătoare ale operațiunilor cibernetice rusești din anii 2010 și începutul anilor 2020, privite printr-o lentilă politico-strategică. Aceasta documentează sistematic modul în care Rusia a planificat și a executat principalele sale campanii cibernetice și le corelează cu obiectivele sale geopolitice. O asemenea contribuție empirică îmbogățește înțelegerea comportamentului strategic al Rusiei și evidențiază rolul serviciilor de informații și al unităților cibernetice în derularea politicii externe a statului rus în spațiul digital.
- **Inovație metodologică:** Prin aplicarea metodologiei de comparație structurată a studiilor de caz (conform modelului Van Evera) la domeniul conflictelor cibernetice, teza demonstrează utilitatea abordării calitative riguroase în studierea războiului cibernetic. Se arată că metodele calitative pot fi aplicate cu succes într-un domeniu adesea dominat de analize tehnice, ceea ce încurajează o examinare mai teoretică a incidentelor cibernetice. Această abordare validată constituie o contribuție la design-ul cercetării în studiile de securitate, ilustrând modul în care testarea ipotezelor în mod calitativ poate fi fructificată în contextul securității cibernetice.
- **Implicații pentru politici și teorie:** Constatările tezei au implicații atât pentru decidenții politici, cât și pentru dezvoltarea teoriei relațiilor internaționale. Pentru factorii de decizie, înțelegerea cyber intelligence-ului ca multiplicator de forță subliniază necesitatea consolidării apărării cibernetice și a capacităților de contrainformații; statele trebuie să conștientizeze că și adversarii aparent mai slabi pot provoca daune semnificative sau pot exercita o influență disproporționată prin mijloace cibernetice. Pentru teoria relațiilor internaționale, cercetarea sugerează că teoriile existente despre putere (în special perspectivele realiste asupra echilibrului de putere și ale descurajării) ar trebui actualizate pentru a include dimensiunea cibernetică. Noțiunea de descurajare, de pildă, devine mai complexă atunci când acțiunile cibernetice ascunse estompează granița dintre război și pace. În acest fel, teza oferă o perspectivă originală asupra integrării dimensiunii cibernetice în conceptele de putere națională și securitate.

Concluzii și relevanță: Cazul Rusiei ilustrează tendința generală conform căreia cyber intelligence-ul a devenit o componentă indispensabilă a dinamicii puterii în epoca modernă. Teza concluzionează că, atunci când sunt exploatate eficient, operațiunile de intelligence cibernetic acționează ca un veritabil multiplicator de forță: ele amplifică raza de acțiune și impactul demersurilor unui stat dincolo de ceea ce ar fi posibil prin mijloace convenționale. În sistemul internațional actual, în care marile puteri evită adesea conflictul armat direct din cauza costurilor și riscurilor ridicate, operațiunile cibernetice ocupă o nișă strategică – permițând unor state precum Rusia să urmărească obiective agresive sub acoperirea negării plauzibile și sub pragul declarării formale a războiului. Cercetarea subliniază că dinamica puterii globale evoluează; măiestria într-un domeniu precum cel cibernetic se poate traduce în atuuri diplomatice, capacități coercitive și influență, într-un mod ce contestă ierarhiile convenționale ale puterii. Prin urmare, înțelegerea și integrarea dimensiunii cibernetice atât în practica politicii externe, cât și în teoria relațiilor internaționale, devin esențiale. Lecțiile extrase din experiența Rusiei constituie un reper pentru alți actori statali și pentru cercetători în demersul de a înțelege modul în care se exercită puterea în era digitală, consolidând argumentul central al tezei referitor la rolul transformator al cyber intelligence-ului în politica mondială.