Școala Națională de Studii Politice și Administrative

TEZĂ DE DOCTORAT

Apărarea cibernetică în contextul războiului hibrid. Studiu comparativ

REZUMAT

Coordonator științific

Prof. Univ. Dr. Teodor MELEȘCANU

Doctorand

Drd. Claudiu-Mihai CODREANU

București

2022

Cuprins

Rezumat

Introducere

De la primele *malware* apărute în secolul trecut și de la primele preocupări legate de posibilitatea unui război cibernetic (chiar și de când era doar subiect pentru literatură științifico-fantastică), din 2007 până în prezent, operațiunile cibernetice au devenit un element aproape central în acțiunile actorilor statali la nivel internațional, mijloacele cibernetice fiind acum esențiale pentru majoritatea domeniilor. În 2007, atacurile cibernetice care au paralizat infrastructura digitală a Estoniei au reprezentat o premieră, mai ales că operațiunea a fost lansată de un alt actor statal, Federația Rusă. Tot Rusia a mai provocat o premieră în 2008, atunci când a utilizat într-o campanie integrată operațiuni cibernetice cu operațiunile cinetice în timpul războiului ruso-georgian din 2008. Totuși, nu doar Rusia a deschis calea utilizării atacurilor cibernetice de către state. În 2009-2010, Statele Unite au utilizat malware-ul Stuxnet împotriva Iranului, țintind o unitate de îmbogățire a uraniului într-o campanie coordonată pentru a preveni dezvoltarea armamentului nuclear de către statul iranian. În următorii ani, atacurile cibernetice au început să fie integrate în campanii cibernetice, integrate apoi în campanii de influențare hibridă care includeau mai multe mijloace. Alte premiere au avut loc în 2015, odată cu atacurile cibernetice ale Rusiei împotriva rețelei de distribuție de energie electrică a Ucrainei și în 2017, odată cu atacul cibernetic NotPetya al Rusiei împotriva Ucrainei, și cu campania cibernetică globală nord-coreeană WannaCry, care a avut un impact serios asupra spitalelor din Regatul Unit. Totodată, în 2020-2021 au avut loc și două campanii majore de spionaj cibernetic, care au generat un răspuns semnificativ din partea Statelor Unite (cele două campanii fiind atribuite public Rusiei și Chinei).

Operațiunile cibernetice ale actorilor statali împotriva statelor din spațiul euroatlantic au devenit din ce în ce mai frecvente, dar doar o parte din acestea pot fi considerate majore, acestea fiind și cele care au avut efecte disruptive semnificative, au fost atribuite public de statele afectate, iar în unele cazuri au fost chiar subiectul unor sancțiuni internaționale. Până în prezent, Federația Rusă a utilizat împotriva statelor euro-atlantice toată seria de operațiuni cibernetice, de la atacuri cibernetice disruptive, la spionaj cibernetic. Pentru Rusia, Ucraina a reprezentat ținta principală a operațiunilor cibernetice ofensive, ținând cont atât de desfășurarea războiului ruso-ucrainean și de agresiunile hibride împotriva Ucrainei, cât și de vulnerabilitățile statului ucrainean. Dacă atacul cibernetic Stuxnet a fost primul atac distructiv major îndreptat împotriva infrastructurii energetice, atacurile cibernetice rusești asupra rețelei de distribuție a

energiei electrice din Ucraina au reprezentat primele atacuri cibernetice disruptive care au vizat afectarea populației civile. În plus, campania cibernetică NotPetya a provocat pagube semnificative în Ucraina, și reprezintă operațiunea cibernetică cu cele mai mari pagube la nivel global. Totuși, un avantaj strategic al utilizării operațiunilor cibernetice este păstrarea ambiguității cu privire la obiective și la actorii responsabili, aceste elemente fiind centrale pentru mijloacele războiului hibrid. Astfel, odată ce operațiunile cibernetice au început să fie utilizate de actorii statali cu scopuri politice, statele au început să își consolideze apărarea și securitatea cibernetică, adoptând în anii 2000 primele strategii naționale de securitate cibernetică și începând să își organizeze instituțiile pentru a putea răspunde activităților cibernetice malițioase. Actorii internaționali din spațiul euro-atlantic au răspuns campaniilor cibernetice atât prin atribuirea publică colectivă a operațiunilor cibernetice și sancționarea statelor respective, cât și prin propriile operațiuni cibernetice ofensive, argumentând că acestea au un caracter defensiv.

Design-ul metodologic

Argumentul cercetării este că activitățile malițioase desfășurate în și prin spațiul cibernetic, la fel și spațiul cibernetic în sine, au o importanță majoră pentru Relațiile Internaționale, mijloacele cibernetice fiind integrate în cadrul campaniilor hibride ale actorilor statali. Totodată, operațiunile cibernetice ofensive lansate de actori statali precum Rusia sau China fac parte dintr-o campanie coordonată și integrată de activități cibernetice malițioase cu scopuri politice, campanie la rândul ei integrată în cadrul unei campanii hibride, care are ca obiectiv subminarea statelor, instituțiilor statelor, proceselor democratice și dezbinarea societăților în țările țintite. Astfel, în contextul acestor campanii hibride și campanii de operațiuni cibernetice, apărarea cibernetică devine esențială pentru securitatea statelor euro-atlantice, dar acestea trebuie să țină cont și de valorile democratice în elaborarea unor răspunsuri în fața operațiunilor cibernetice, existând și o confruntare între democrații și modelul autoritarismului digital adoptat și promovat de state ca Rusia și China.

Cercetarea încearcă să răspundă la două întrebări de cercetare principale: În ce mod au fost utilizate operațiunile cibernetice ofensive de către Rusia și alți actori statali împotriva statelor din spațiul euro-atlantic?; Ce fel de măsuri au implementat statele euro-atlantice pentru a asigura apărarea și securitatea cibernetică?. Așadar, studiul va pleca de la două ipoteze:

1. *Operațiunile cibernetice ofensive majore lansate de Rusia și de alți actori statali împotriva statelor din spațiul euro-atlantic sunt utilizate în cadrul unor campanii cibernetice (nefiind incidente izolate) și sunt integrate în cadrul unor mijloace și*

campanii hibride de influențare și subminare a statelor respective, specifice autoritarismului digital.

2. *Apărarea și securitatea cibernetică sunt centrale pentru eforturile actorilor statali din spațiul euro-atlantic de a răspunde campaniilor hibride lansate de Rusia și de alți actori statali.*

În studierea conflictului cibernetic și al modalităților în care tehnologiile digitale sunt folosite în contexte politice de către actori statali și nu numai, atenția a început să treacă de la studierea unor scenarii teoretice de atacuri cibernetice „apocaliptice" (de tipul „Pearl Harbor cibernetic") către scenarii care iau în calcul realitatea operațiunilor cibernetice continue de intensitate scăzută cuprinse în diferite contexte de conflicte (Dunn Cavelty și Wenger 2020, pp. 14-20). Conform lui Lucas Kello (2017), cercetătorii din domeniile Relațiilor Internaționale și ale studiilor de securitate sunt sceptici cu privire la existența și importanța amenințărilor cibernetice. Totuși, cercetările legate de evoluțiile din spațiul cibernetic, tehnologie și știință, care fac legătura cu politica nu mai sunt rare în Relațiile Internaționale și studiile de securitate (Dunn Cavelty și Wenger 2020, p. 6).

Studiul va lua ca reper statele euro-atlantice, urmărind impactul operațiunilor cibernetice majore lansate de actori statali împotriva Statelor Unite, Regatului Unit, Germaniei și Ucrainei. În plus, cercetarea privind apărarea cibernetică și analiza strategiilor naționale de securitate cibernetică va include atât SUA și Regatul Unit, cât și Estonia și Uniunea Europeană, chiar dacă cea din urmă nu reprezintă un actor statal. În cea mai mare parte, cercetarea se va axa pe abordările școlii liberale din Relațiile Internaționale (RI), dar va ține cont și de concepte și teorii din cadrul altor școli RI, literatura de specialitate utilizată fiind variată din punctul de vedere al curentelor din RI. Studiile de caz reprezintă o explorare a operațiunilor cibernetice ofensive lansate împotriva statelor euro-atlantice, urmărind patru studii de caz elocvente, diferite și similare în anumite aspecte, explorate prin desfășurarea atacurilor, impactul acestora și modalitatea desfășurării apărării cibernetice. Operațiunile cibernetice pe care se axează cercetarea sunt cele realizate de actori statali împotriva altor actori statali, dar care au fost făcute posibile prin Internet, nu numai prin utilizarea tehnologiilor digitale sau cibernetice.

Pentru a putea analiza o operațiune cibernetică, trebuie stabilit contextul în care a avut loc acțiunea, trebuie stabilit dacă operațiunile au fost atribuite public către un actor statal, dacă acestea au avut obiective politice și dacă au afectat instituții importante ale statului sau infrastructura critică, intensitatea și complexitatea atacului, impactul asupra societății și a reputației actorului, dar și stabilită legătura cu alte evenimente și verificarea existenței unei campanii cibernetice extinse sau o campanie hibridă mai amplă (Happa și Fairclough 2017;

Steiger et al. 2018; Kello 2017). În conflictele dintre actori statali, războiul cibernetic (set de mijloace utilizat pentru a purta conflicte în și prin exploatarea spațiului cibernetic) poate fi considerat o parte sau o categorie a mijloacelor războiului hibrid. Operațiunile cibernetice sunt folosite în cadrul unui set mai larg de strategii, politici și operațiuni, utilizate ca instrumente de politică externă, cu scopul de a submina securitatea statului respectiv, economia, societatea sau statul în sine. Acest lucru este evidențiat de conflictele cibernetice dintre Rusia și statele euro-atlantice și dintre China și democrațiile liberale. În acest caz, are loc pe de o parte un conflict purtat prin mijloace hibride, unde mijloacele cibernetice sunt utilizate pentru purtarea conflictului dintre state (operațiuni de influență, sabotaj, subminare etc.), dar și un conflict între democrații liberale și regimuri autoritare (democrație digitală versus autoritarism digital).

În cadrul cercetării, războiul hibrid este înțeles ca un set de mijloace și o formă de purtare a conflictelor cu un instrumentar extins. Războiul hibrid reprezintă un amestec de mijloace de purtare a conflictului, integrează o varietate largă de tipuri diferite de conflicte, dar preponderent utilizează mijloace non-militare de interferență, croite pentru a submina statul vizat, intensificarea divizărilor din societatea vizată și slăbirea coeziunii interne, mijloacele hibride reprezentând o strategie sau politică de a slăbi potențialul actorilor țintiți (Wigell 2019; Lasconjarias și Larsen 2015; Hoffman 2007). Operațiunile cibernetice sunt esențiale pentru războiul hibrid, permițând acțiuni coercitive sub pragul războiului convențional (Lewis 2015). În cadrul acestei cercetări voi utiliza terminologia de „război hibrid”, anunțată încă din titlu, dar și cea de campanii hibride. Pe baza conceptualizării realizate de Mikael Wigell (2019) și de alți cercetători (Kello 2021; Rinelli și Duyvesteyn 2017; Reichborn-Kjennerud și Cullen 2016; Hoffman 2009; Lasconjarias și Larsen 2015), prin „război hibrid” mă refer la un set de mijloace, operațiuni, strategii și/sau politici prin care un actor încearcă să influențeze un alt actor pentru a obține obiective politice și de a încerca subminarea statului sau a societății.

Totodată, am luat în considerare în cadrul acestei cercetări strategiile naționale de securitate cibernetică ale Regatului Unit, Statelor Unite, Estoniei, și Uniunii Europene. Regatul Unit și Statele Unite au fost alese pentru acest studiu deoarece sunt actori statali importanți în spațiul cibernetic, cele două state au fost țintele unor atacuri cibernetice majore în ultimii 10 ani, lansând la rândul lor operațiuni cibernetice împotriva altor actori statali și non-statali. La fel, Estonia a fost victima unui atac cibernetic de referință în 2007, iar de atunci statul estonian a pus accentul semnificativ pe construirea unei apărări cibernetice eficiente și solide pentru a preveni noi atacuri, Tallinnul reprezentând un model pentru alte state în ceea ce privește securitatea cibernetică. Am ales și Uniunea Europeană deoarece reprezintă strategia unei organizații internaționale și a unui întreg grup de state, dar și pentru că a fost victimă a

atacurilor cibernetice. În plus, strategia UE pune accentul pe libertățile online ;i pe promovarea unui spațiu cibernetic deschis și global. Strategiile de securitate cibernetică ale celor patru actori internaționali vor fi discutate urmărind principalele amenințări percepute, modalitățile de acțiune pentru asigurarea apărării și securității cibernetice, dar și a accentului pus pe alte măsuri – cooperare internațională, democrație digitală, drepturi digitale. Așadar, apărarea cibernetică reprezintă modul în care statele iau măsuri pentru a preveni sau contracara atacurile și operațiunile cibernetice. Acestea pot include utilizarea de sisteme de securitate cibernetică a rețelelor critice, elaborarea unor planuri clare în domeniul cibernetic și sporirea cooperării interinstituționale și internaționale sau măsuri pentru creșterea culturii de securitate cibernetică a populației.

Astfel, principalele contribuții ale cercetării sunt, în primul rând, analizarea din perspectiva Relațiilor Internaționale a activităților malițioase desfășurate în și prin intermediul spațiului cibernetic, evoluția rolului spațiului cibernetic și a apărării cibernetice pentru actorii statali în contextul utilizării de către state a mijloacelor și campaniilor hibride. Totodată, cercetarea contribuie prin analizarea operațiunilor cibernetice ofensive majore lansate de Rusia și China împotriva statelor euro-atlantice și integrarea acestora într-o campanie coordonată de operațiuni cibernetice, la rândul ei fiind integrată într-o campanie hibridă de subminare a statelor țintite. Prin discutarea principalelor concepte și teorii privind spațiul cibernetic și operațiunile cibernetice din Capitolul 1, studiul contribuie la consolidarea înțelegerii spațiului cibernetic, a operațiunilor cibernetice și a apărării și securității cibernetice în cadrul domeniului Relațiilor Internaționale. În plus, prin analizarea operațiunilor cibernetice majore lansate de actori statali împotriva Ucrainei, SUA, Regatului Unit și Germaniei, studiul contribuie prin consolidarea înțelegerii în cadrul RI a impactului operațiunilor asupra statelor și a modalităților de răspuns pe care le pot avea statele. O altă contribuție importantă a cercetării este creșterea nivelului de înțelegere a modalităților prin care pot fi asigurate și realizate apărarea și securitatea cibernetică, în special prin promovarea unor modele care respectă valorile democratice. Capitolul 3 discută atât modelele democrațiilor din spațiul euro-atlantic, analizând strategiile de securitate cibernetică ale SUA, Regatului Unit, Estoniei și UE, dar și modelele autoritarismului digital (Rusia și China), fiind explorată inclusiv dezbaterea din cadrul ONU privind reglementarea internațională a spațiului cibernetic și a activităților cibernetice, discuțiile din cadrul ONU fiind locul unde se confruntă cele două modele de guvernare.

Structura lucrării

În Capitolul 1, cercetarea va porni de la definirea și discutarea principalelor concepte și termeni privind spațiul cibernetic (operațiuni cibernetice, atacuri cibernetice, spionaj cibernetic, arme cibernetice etc.), dar și discutarea principalelor aspecte ale războiului hibrid, critici aduse conceptului și o conceptualizare a războiului (sau conflictului) cibernetic. Totodată, capitolul include și explorarea principalelor abordări și viziuni din cadrul Relațiilor Internaționale privind spațiul cibernetic, precum discutarea conceptelor de putere cibernetică, descurajare, cooperare internațională, chestiunea atribuirii sau autoritarismul digital și rolul actorilor statali în spațiul cibernetic.

Capitolul 2 explorează, în prima parte, principalele operațiuni cibernetice care au avut loc după 2000 și evoluția operațiunilor cibernetice ale Rusiei, Chinei, Statelor Unite, Coreei de Nord și Iranului. În cea de-a doua parte, capitolul include analizarea operațiunilor cibernetice majore lansate de actori statali împotriva a patru state din spațiul euro-atlantic (Ucraina, Statele Unite, Regatul Unit și Germania), ținând cont de statul căruia i-a fost atribuită operațiunea cibernetică. Principalele state care utilizează spațiul cibernetic și armele cibernetice ca mijloc de subminare a democrațiilor sunt China și Rusia, dar accentul principal va fi pus pe operațiunile Rusiei, acestea fiind integrate în campanii hibride împotriva statelor țintite. Cercetarea se va axa în principal pe operațiunile cibernetice asupra rețelei electrice a Ucrainei, pe atacul cibernetic NotPetya și pe campania cibernetică a Rusiei împotriva SUA din 2016.

Capitolul 3 urmărește modul în care o parte din statele din spațiul euro-atlantic și-au dezvoltat strategii și politici de a combate activitățile malițioase din spațiul cibernetic, fiind discutate principalele aspecte ale strategiilor de securitate cibernetică ale patru actori internaționali: Statele Unite, Regatul Unit, Estonia și Uniunea Europeană, urmărind modul în care cei patru actori își propun asigurarea apărării și securității cibernetice. În plus, cercetarea include și discutarea modelelor de apărare cibernetică a Rusiei și Chinei – modelul autoritarismului digital – și dezbaterea dintre autoritarismul digital și democrația digitală din cadrul discuțiilor ONU privind reglementarea spațiului cibernetic.

În Capitolul 4, studiul se axează pe discutarea spațiului cibernetic în cadrul Relațiilor Internaționale și evoluțiile acestuia în contextul războiului hibrid. Capitolul include analizarea operațiunilor cibernetice ofensive ale Chinei și Rusiei, și încadrarea operațiunilor Rusiei desfășurate împotriva actorilor euro-atlantici în cadrul mijloacelor unor campanii hibride. În plus, cercetarea include și o discuție privind apărarea cibernetică a statelor euro-atlantice, punând accentul pe rolul măsurilor și răspunsurilor luate, de la atribuiri publice și sancțiuni, la operațiuni cibernetice ofensive sau la creșterea rezilienței cibernetice și a cooperării

internaționale. În final, capitolul include și o serie de recomandări pentru asigurarea apărării și securității cibernetice.

Rezultate și discuții

Tehnologiile trebuie să fie luate în calcul ca fiind inseparabile față de politică și vice-versa. Desfășurarea politicii în spațiul cibernetic a generat efecte la nivel global, formându-se interese noi, schimbări în discursul politic și interacțiuni, dar și noi modele de înțelegeri globale și răspunsuri instituționale. Spațiul cibernetic oferă noi mijloace și locuri în care statele să-și poată exercita puterea, oferind și posibilitatea de a pune accentul pe suveranitate și teritorialitate în justificarea activităților. Totodată, spațiul cibernetic le-a permis indivizilor și organizațiilor să comunice și să se organizeze în moduri care nu erau posibile până atunci, ceea ce a generat provocări pentru conceptele tradiționale asupra suveranității. (Choucri 2012, pp. 10-14; Dunn Cavelty și Wenger 2022, p. 2)

Așadar, securitatea cibernetică reprezintă un tip de securitate care se desfășoară „în și prin intermediul spațiului cibernetic", astfel că practicile de securitate cibernetică sunt constrânse și permise de acest mediu (Balzacq și Dunn Cavelty 2016, p. 179). În plus, Thierry Balzacq și Myriam Dunn Cavelty (2016, p. 183) definesc securitatea cibernetică drept un „set de practici elaborate pentru a proteja rețelele, calculatoarele, programele și datele de atacuri, pagube sau acces neautorizat", practicile reprezentând acțiuni luate de diferiți actori pentru a face spațiul cibernetic mai sigur. Conform lui Lucas Kello (2017, p. 46), securitatea cibernetică se referă la măsurile necesare pentru a proteja spațiul cibernetic de acțiuni ostile, dar și ca absența intruziunilor neautorizate în sistemele de calculatoare și buna funcționare a acestora.

În dezbaterea și confruntarea dintre autoritarismul digital și democrație, democrațiile liberale par să se fi erodat în ultimii 15 ani, în timp ce autoritarismul digital se extinde, devenind mai agresiv și mai ofensiv. Acest lucru a fost evidențiat în studiul modelului de apărare cibernetică și de autoritarism digital al Rusiei și Chinei din Capitolul 3, dar și în analiza operațiunilor cibernetice care au țintit democrațiile din spațiul euro-atlantic din Capitolul 2. Rusia, China, Iran și Coreea de Nord au desfășurat o serie (sau chiar campanie) semnificativă de operațiuni cibernetice împotriva democrațiilor din spațiul euro-atlantic, având ca obiective atât riposta pentru diferite acțiuni ale acestora, dar și subminarea proceselor, valorilor și instituțiilor democratice, dezbinarea societăților democratice, perturbarea activităților economice și provocarea de perturbări pentru cetățeni, afaceri, societate civilă sau guvern. Rusia a lansat toate tipurile de operațiuni cibernetice împotriva statelor euro-atlantice, majoritatea împotriva Ucrainei, de la spionaj cibernetic, atacuri cibernetice care au provocat

pagube materiale considerabile și care au afectat buna funcționare a infrastructurii critice și altele care au avut scopul de a submina statul, societatea și cursul politicii externe și interne a statului (de la intruziuni, infiltrări, intruziuni cibernetice urmate de scurgeri de informații și campanii informaționale, atacuri tip DDoS etc.). În ceea ce privește acțiunile cibernetice ale Rusiei împotriva celorlalte state euro-atlantice, excluzând Ucraina, Rusia s-a axat pe campanii de spionaj cibernetic și operațiuni cibernetice dublate de campanii de dezinformare prin care a încercat subminarea proceselor electorale și altor elemente ale democrației, subminarea încrederii în stat și instituții și dezbinarea societății, precum și schimbarea cursului de politică externă al statelor.

În schimb, China s-a concentrat pe spionajul cibernetic, vizând ținte economice, industriale și militare majore (cu precădere în SUA și în statele NATO), dar Beijingul nu a fost găsit responsabil pentru operațiuni cibernetice ofensive cu scopuri distructive sau disruptive, chiar dacă unele intruziuni și infiltrări cibernetice realizate în contextul unor campanii de spionaj au provocat pagube colaterale. China joacă un rol foarte important în spațiul cibernetic, atât în ceea ce privește utilizarea operațiunilor cibernetice, cât și în ceea ce privește controlul asupra tehnologiei și a industriei tehnologice, ceea ce are impact la nivel global. Beijingul a preferat să întrețină în special campanii de spionaj cibernetic împotriva statelor din spațiul euroatlantic, atacurile cibernetice cu scopuri disruptive sau chiar distructive fiind aproape inexistente, iar accentul a fost pus aproape exclusiv pe spionaj. China utilizează frecvent operațiuni cibernetice pentru a îndeplini obiective legate de spionaj, extrăgând informații sensibile pentru a obține avantaje industriale și comerciale. În schimb, Rusia s-a axat pe lansarea de operațiuni cibernetice pentru a submina afacerile interne ale altor state (Kello 2018, p. 666). Chiar dacă intensitatea operațiunilor cibernetice ale guvernului chinez a fost ceva mai redusă, acestea rămân importante, așa cum este cazul campaniei de spionaj cibernetic împotriva SUA din 2020-2021 (hack-ul împotriva Microsoft Exchange). Așadar, operațiunile de spionaj cibernetic ale Chinei, care au vizat cu precădere Statele Unite, fac parte dintr-o campanie amplă a Chinei și nu reprezintă incidente izolate, afectează reputația SUA, și au extras date importante, au o complexitate ridicată și obiective politice, dar nu au avut efecte majore asupra societății, comparabil cu campaniile cibernetice ale Rusiei. Spre exemplu, campaniile SolarWinds și Microsoft Exchange au reprezentat campanii de spionaj cibernetic, dar operațiunile cibernetice care au stat la baza activităților de spionaj au depășit o limită de acceptabilitate pentru guvernul SUA și pentru partenerii internaționali, operațiunile de spionaj cibernetic având o amploare și o profunzime mult prea mare pentru a putea fi tolerate, în timp ce breșele de securitate create în cursul infiltrărilor cibernetice au lăsat în urmă vulnerabilități

serioase care puteau fi exploatate de orice alt actor cu scopuri distructive. Chiar dacă nu a avut un scop distructiv, ci doar de spionaj, aceasta a presupus incursiuni majore în sectoare guvernamentale critice și accesul unor informații secrete importante.

Totodată, Iranul este considerat un actor semnificativ în spațiul cibernetic, dar operațiunile cibernetice ofensive desfășurate au fost mult mai rare față de cele ale Chinei și Rusiei, Iranul axându-se pe spionaj cibernetic și pe operațiuni cibernetice ofensive lansate ca ripostă (precum cele împotriva Arabiei Saudite, Statelor Unite sau Israelului). În ultimul rând, Coreea de Nord, un stat mic dar cu capabilități cibernetice considerabile, s-a axat pe operațiuni specifice mai degrabă criminalității cibernetice, cum au fost atacurile tip ransomware și intruziuni împotriva băncilor și a instituțiilor financiare (urmărindu-se extragerea de fonduri), dar și o operațiune cibernetică majoră împotriva unei companii private din SUA (Sony Pictures). Coreea de Nord a provocat și unul dintre cele mai semnificative și ample atacuri cibernetice din istorie, WannaCry, un atac tip ransomware care a scăpat de sub control și a provocat pagube colaterale de miliarde de dolari, afectând puternic și sistemul de spitale din Regatul Unit, chiar dacă scopul inițial al atacului ar fi fost doar obținerea de răscumpărări de la organizațiile afectate.

În schimb, operațiunile cibernetice ale Rusiei împotriva actorilor euro-atlantici au ca scop îndeplinirea unor obiective de politică externă și influențarea statelor țintite, operațiunile cibernetice și acțiunile hibride fiind percepute ca un mecanism de apărare împotriva statelor adversare și de destabilizare internă a acestora. Campaniile cibernetice au permis Rusiei să încerce prin acțiuni non-violente perturbarea cursului politicilor interne și externe ale unui stat, evitând anumite pedepse și desfășurând acțiunile sub pragul războiului. Operațiunile cibernetice sunt lansate cu scopul de a avansa aspirațiile geopolitice ale Moscovei, încercând să distragă și să destabilizeze Occidentul până în punctul în care nu mai poate combate eficient acțiunile Rusiei, să submineze guvernele și organizațiile din spațiul euro-atlantic percepute drept ostile, dar și să încerce să își impună sau consolideze dominanța în spațiul ex-sovietic și să încerce revendicarea statutului de mare putere (Limnell 2018, p. 67).

Operațiunile cibernetice ale Rusiei lansate după 2007 împotriva Estoniei, Georgiei, Ucrainei, Franței, Germaniei, Statelor Unite, Regatului Unit etc. reprezintă elemente ale unei campanii mai largi a Rusiei de a submina încrederea publică și coeziunea și securitatea statelor europene, dar și să submineze Uniunea Europeană și NATO, crescând inclusiv costurile eforturilor de aderare la cele două organizații (Kello 2021; Wilner 2019). Astfel, operațiunile cibernetice discutate în cadrul Capitolului 2 au fost atribuite public unor actori statali, majoritatea au avut obiective politice, au afectat instituții importante, procese democratice și

infrastructura critică, operațiunile au fost complexe și sofisticate (în special NotPetya sau campania de spionaj SolarWinds), intensitatea și amploarea NotPetya și WannaCry ieșind în evidență, au avut un impact semnificativ asupra societății dar și a reputației actorilor afectați, și pot fi toate încadrate în cadrul unei campanii hibride ample a statelor care promovează modelul autoritarismului digital.

Spre exemplu, operațiunile cibernetice ale Rusiei împotriva alegerilor prezidențiale din SUA din 2016 au fost complexe și sofisticate, au avut o intensitate mare, au subminat democrația liberală, au avut obiective politice clare, au avut un impact major asupra societății și a statului și fac parte dintr-o campanie cibernetică mai largă a Rusiei împotriva SUA și a statelor euro-atlantice, dar și dintr-o campanie mai extinsă de operațiuni hibride ale Rusiei împotriva statelor euro-atlantice, activitățile malițioase ale Rusiei vizând o parte semnificativă din aceste state, obiectivele fiind similare. Acestea au fost corelate și cu campanii de dezinformare și cu mai multe mijloace hibride, fiind o campanie hibridă integrată și coordonată care a vizat subminarea proceselor democratice, dezbinarea societății și interferarea în alegerile americane. În acest context, răspunsul SUA a constat în atribuiri publice realizate în cadrul unor coaliții internaționale, impunerea de sancțiuni, punerea sub acuzare a mai multor agenți de informații ruși, dar și prin lansarea unor operațiuni cibernetice ofensive. Campania hibridă Rusiei a reprezentat o încercare de a dezbina societatea americană și de a schimba soarta alegerilor, modelând un mediu geopolitic în care Rusia putea opera.

Mai mult, operațiunile cibernetice ale Rusiei împotriva Ucrainei au fost integrate într-o campanie hibridă extinsă a Rusiei împotriva Ucrainei, care a inclus și anexarea ilegală de teritorii și întreținerea războiului din Donbas (inclusiv prin participarea trupelor ruse, nu doar prin sprijinirea forțelor separatiste). Atacurile cibernetice ale Rusiei împotriva rețelei electrice ucrainene din 2015-2016 au reprezentat o premieră, la fel și nivelul de sofisticare și complexitate al acestora. Operațiunile au afectat societatea ucraineană, au subminat autoritățile ucrainene și statul, obiectivele operațiunii fiind politice. Totodată, acestea s-au încadrat într-o campanie largă de operațiuni cibernetice lansate împotriva Ucrainei, de la primele atacuri împotriva instituțiilor guvernamentale și a procesului electoral din 2014, până la atacul cibernetic NotPetya din 2017. Atacul NotPetya reprezintă unul dintre cele mai complexe și extinse atacuri cibernetice din istorie, fiind și cel mai costisitor. Operațiunea cibernetică a Rusiei a avut obiective politice și a vizat subminarea statului ucrainean și a economiei, afectând reputația statului, atacul afectând companiile private și de stat ucrainene (și instituțiile publice), dar și companiile private care aveau afaceri în Ucraina. În plus, în timpul reînnoirii invaziei rusești a Ucrainei din 2022, Rusia a corelat atacurile cibernetice cu operațiunile cinetice

(Microsoft 2022). Operațiunile cibernetice trebuie să fie încadrate în contextul întregului conflict ruso-ucrainean. Astfel, și în cazul acestor operațiuni cibernetice, scopul Rusiei pare să fi fost mai degrabă să submineze statul ucrainean, societatea, democrația și economia și să le slăbească. Incidentele cibernetice înregistrate în Ucraina au îndeplinit obiectivul principal al războiului hibrid, îndeplinind obiective politice fără a provoca un răspuns al adversarului prin utilizarea de metode de intensitate scăzută pentru a menține acțiunile sub pragul războiului, acestea oferind un flux constant, stabil și intens de perturbări ale activităților guvernului, societății și economiei Ucrainei (Rõigas 2017, pp. 242-243).

În schimb, operațiunile cibernetice ale Rusiei în Germania și Regatul Unit au avut o intensitate mai redusă față de Ucraina sau SUA, chiar dacă obiectivele interferențelor cibernetice în procesele electorale din cele două țări au fost tot politice. Germania a reprezentat o țintă a campaniilor cibernetice și informaționale ale Rusiei, dar cea mai semnificativă operațiune a avut loc în 2015. De atunci, interferarea în alegerile legislative din 2017 și 2021 a fost prevenită în urma răspunsurilor substanțiale de apărare cibernetică adoptate de Germania după 2015, precum atribuirea atacurilor din 2015 și condamnarea acestora, dialogul cu Rusia și luarea de măsuri pentru creșterea securității cibernetice a proceselor electorale și a instituțiilor de stat. Cu toate acestea, autoritățile au identificat activități cibernetice malițioase ale Rusiei în contextul alegerilor din 2021, au atribuit campania Rusiei, dar acestea au avut efecte marginale. În schimb, Regatul Unit a fost vizat de campania hibridă a Rusiei de a submina procesele electorale ale statelor din spațiul euro-atlantic, existând suficiente indicii că Rusia a utilizat operațiuni cibernetice și informaționale în timpul campaniei pentru Brexit, chiar dacă efectele tentativelor de interferare în alegerile legislative din 2017 au fost neglijabile.

Astfel, operațiunile cibernetice ofensive majore lansate de Rusia au fost recunoscute, atribuite public și încadrate către SUA, UE și statele partenere în cadrul unor campanii cibernetice coordonate ale Rusiei împotriva statelor țintite. În plus, campaniile cibernetice ale Rusiei sunt integrate în cadrul campaniilor hibride de influență și interferare în statele euro-atlantice vizate, obiectivele fiind subminarea proceselor democratice, instituțiilor și guvernelor, dezbinarea societăților, scăderea încrederii populației în stat și perturbarea activităților mediului economic, al industriei și al societății. În schimb, China s-a concentrat pe campanii semnificative de spionaj cibernetic, obiectivele principale fiind colectarea de intelligence, chiar dacă și activitățile cibernetice malițioase ale Chinei sunt încadrate de statele euro-atlantice în cadrul unor campanii cibernetice mai largi, și pot fi încadrate într-o campanie integrată de a consolida și promova autoritarismul digital (la fel ca în cazul Rusiei). Totodată, state ca Iran și Coreea de Nord reprezintă actori importanți în domeniul cibernetic, dar operațiunile cibernetice

lansate au fost sporadice și nu au produs efecte la fel de mari ca cele ale Rusiei, și nici nu au reușit să extragă informații atât de importante ca operațiunile de spionaj ale Chinei. Totuși, și operațiunile cibernetice ale acestora pot fi încadrate în cadrul unor campanii ofensive a autoritarismului digital, scopul acțiunilor fiind tot subminarea democrației și a statelor țintite. Statele autoritare încearcă să controleze spațiul cibernetic și informațional pentru a-și proteja regimurile, promovând și reglementări la nivel global care să corespundă propriilor viziuni, dar și prin utilizarea tehnologiilor digitale pentru a-și controla propria populație și pentru a submina statele considerate adversare (Barrinha și Renard 2020; Polyakova și Meserole 2018; Yayboke și Brannen 2020). Așadar, interferența hibridă reprezintă o amenințare semnificativă la adresa democrațiilor liberale, considerând elementele democratice drept vulnerabilități care pot fi exploatate pentru a diviza societățile și pentru a submina guvernarea (Wigell 2019, p. 256).

În acest context internațional privind spațiul cibernetic, statele euro-atlantice au adoptat sau și-au propus obiective semnificative de apărare cibernetică, scopul fiind promovarea și consolidarea securității cibernetice. În ceea ce privește strategiile de securitate cibernetică discutate în cadrul Capitolul 3, toate cele patru strategii (SUA, Regatul Unit, Estonia și UE) au percepții similare asupra amenințărilor și riscurilor provenite din spațiul cibernetic, și toți cei patru actori pun accentul pe respectarea valorilor democratice și a drepturilor omului în timpul elaborării și implementării răspunsurilor și măsurilor de apărare și securitate cibernetică. Modelele Regatului Unit și ale Statelor Unite de apărare și securitate cibernetică pun, totodată, accentul și pe apărarea activă, deci și pe operațiuni cibernetice ofensive cu caracter defensiv. În schimb, Estonia pune accentul pe consolidarea rezilienței cibernetice și a cooperării internaționale. În mod similar, și UE se axează pe obiective similare cu cele estoniene, promovarea unui model democratic de guvernare a Internetului și cooperarea internațională atât cu actori statali și organizații internaționale fiind văzute ca esențiale pentru asigurarea securității cibernetice la nivelul UE și la nivel global.

Apărarea și securitatea cibernetică au devenit centrale pentru eforturile actorilor din spațiul euro-atlantic de a răspunde campaniilor hibride ale Rusiei și ale altor actori statali. Actorii euro-atlantici depun eforturi pentru a-și consolida în interior securitatea și reziliența cibernetică, dar și pentru a spori cooperarea interstatală, atât pentru creșterea capabilităților cibernetice, dar și pentru a oferi răspunsuri colective împotriva operațiunilor cibernetice ofensive, precum realizarea unor atribuiri colective sau impunerea de sancțiuni. Răspunsul față de amenințările și atacurile cibernetice nu trebuie să fie în mod necesar tot de natura unor represalii cibernetice. Atribuirea publică a actorilor care au lansat atacul și impunerea de sancțiuni internaționale, mai ales împreună cu alte state, a fost modalitatea de răspuns preferată

a statelor euro-atlantice după 2015. Mai mult, actorii euro-atlantici încearcă să se concentreze și pe respectarea și promovarea valorilor democratice, atât în ceea ce privește formularea răspunsurilor împotriva activităților cibernetice malițioase, cât și în promovarea unui model democratic de guvernare a spațiului cibernetic, ca alternativă la modelul autoritarismului digital promovat și adoptat de China și Rusia.

La cel mai fundamental nivel, apărarea cibernetică (sau apărarea rețelelor și a sistemelor) presupune utilizarea unor software-uri care scanează automat după coduri malițioase și analiști care monitorizează activ căutând breșe de securitate și intruziuni în rețelele potențialilor adversari pentru a obține intelligence legat de capabilitățile și intențiile acestora (Buchanan 2016, p. 158). În plus, statele trebuie să deruleze un audit de securitate cu privire la sistemele cibernetice guvernamentale și la securitatea rețelelor și a sistemelor clasificate, fiind foarte important să desfășoare analize constante pentru a depista vulnerabilități în sistemele și rețelele informatice (Polyakova și Boyer 2018, pp. 16-30). Totodată, Joe Burton și Claire Lain (2020, p. 16) argumentează că conceptul infrastructurii critice ar trebui să fie extins, fiind nevoie să fie incluse procesele democratice, sectorul educației, grupurile identitare (etnice, religioase sau de gen), mișcările și rețelele sociale.

Astfel, statele vizate de agresiuni hibride în mod sistematic ar trebui să analizeze și să numească acțiunile ca un set de activități ofensive coordonate, impunând pedepse întregii campanii strategice, și nu doar unor acțiuni individuale izolate. Statele trebuie să ia măsuri punitive împotriva unor serii sau campanii de operațiuni cibernetice și nu a unor cazuri individuale, să utilizeze măsuri intersectoriale atunci când pedepsesc operațiuni cibernetice (de la sancțiuni economice și financiare în locul celor individuale la deteriorarea relațiilor comerciale), dar și să ofere un mesaj clar că au capacitatea și voința de a riposta cibernetic (Kello 2021, pp. 12-13). Spre exemplu, SUA și Regatul Unit au început încă din 2017 să prefere atribuirea și observarea unor campanii întregi de intruziuni cibernetice, și nu doar atribuirea unor incidente specifice (Egloff 2020, p. 6).

Așadar, una dintre cele mai importante metode de descurajare și reacție la operațiunile cibernetice ofensive este atribuirea publică a operațiunilor, în special atunci când este făcută în cooperare de mai multe state. Atribuirea publică a operațiunilor cibernetice are în primul rând scopul de coerciție și de descurajare, asigurând că adversarul trebuie să consume mai mult timp și resurse pentru a-și îmbunătăți capabilitățile. În plus, două alte obiective ale atribuirii publice sunt prevenirea și apărarea, iar diseminarea publică a informațiilor privind anumite amenințări va determina operatorii rețelelor să soluționeze rapid problemele de securitate și să asigure o reziliență mai mare a sistemelor. (Egloff și Smeets 2021, pp. 6-7)

După 2017, numărul atribuirilor publice realizate de state a crescut semnificativ, inclusiv atribuirile colective și coordonate. Statele au început să atribuie public operațiuni cibernetice care au fost mai nesemnificative ca amploare față de atacuri cibernetice din trecut, ceea ce indică faptul că atacuri similare cu cele de dinainte de 2018 vor avea șanse mult mai mari să fie atribuite și vor primi un răspuns mai serios. În plus, atribuirea publică reprezintă și o ocazie pentru ca statele să invoce dreptul internațional și normele internaționale (inclusiv normele stabilite de Grupul de Experți Guvernamentali al ONU) ca răspuns la un atac cibernetic.

În plus, statele nu pot asigura securitatea cibernetică singure, iar astfel acestea ar trebui să sporească eforturile de a consolida cooperarea internațională, urmărind să ajungă la o înțelegere pentru un cadru stabil al guvernării spațiului cibernetic și asupra unor norme pentru comportamentul responsabil al statelor (Dunn Cavelty și Wenger 2020, p. 23). Totodată, statele ar trebui să sprijine cooperarea internațională, inclusiv prin schimburi frecvente și dialoguri cu alte state, mai ales înaintea alegerilor cele mai importante (Polyakova și Boyer 2018, p. 32). Statele trebuie să consolideze reziliența cibernetică la nivel global prin parteneriate cu alți actori statali și cu organizații regionale sau internaționale (OSCE, NATO, Uniunea Africană etc.), și inclusiv cu actori din sectorul privat (Pawlak 2018, p. 113). Astfel, statele trebuie să sprijine platforme alternative de dialog la nivel internațional privind chestiunile legate de spațiul cibernetic (Pawlak 2018, p. 114). În lipsa unor acorduri bilaterale semnificative, a unor măsuri de consolidare a încrederii sau a unor înțelegeri la nivel global, chiar și dezvoltarea unor canale de comunicații între actorii statali cu capabilități cibernetice majore (precum SUA, Regatul Unit, China și Rusia) pot contribui la creșterea nivelului de securitate și stabilitate (Buchanan 2016, p. 166).

Ținând cont de faptul că spațiul cibernetic reprezintă un domeniu transfrontalier dar puternic reglementat de anumite guverne, cooperarea internațională are un impact semnificativ și pozitiv pentru asigurarea securității și apărării cibernetice. Cooperarea internațională este importantă atât între principalele state cu roluri importante în spațiul cibernetic (principalele puteri cibernetice), dar și în contextul formării unui bloc de state care promovează autoritarismul digital pe model chinezesc sau rusesc, democrațiile liberale trebuind să își construiască propriul model și propriul bloc de state care să promoveze democrația digitală la nivel internațional. Cooperarea internațională în ceea ce privește spațiul cibernetic trebuie consolidată și sporită, în special în cadrul discuțiilor purtate în GGE al ONU, iar acest lucru ar putea fi posibil, ținând cont că actorii din spațiul cibernetic deja cooperează în ceea ce privește chestiunile tehnice, respectând standardele ICANN sau serverele DNS de bază și infrastructura

centrală a Internetului (Nye 2018; Kello 2021). Mai mult, există și un oarecare consens în cadrul discuțiilor purtate în GGE al ONU, dar discuțiile trebuie intensificate pentru a putea obține un set de norme acceptate de toți actorii statali și de care să țină cont.

În plus, chiar dacă spațiul cibernetic pare să favorizeze ofensiva cibernetică (Isnarti 2016; Slayton 2017), statele trebuie să pună accentul pe apărarea cibernetică și pe acțiuni de descurajare, promovând inclusiv adoptarea unui regim internațional al spațiului cibernetic și respectarea normelor de comportament al statelor în acest domeniu. Mai mult, chiar dacă sunt foarte ridicate costurile lansării unui atac cibernetic complex și sofisticat, costurile apărării cibernetice sunt și mai ridicate (Kello 2017, pp. 68-74). În spațiul cibernetic, apărătorii cibernetici ar trebui să plece de la premisa că adversarii se află deja înăuntrul sistemelor pe care încearcă să le protejeze. Statele Unite și-au asumat mai multe operațiuni ofensive în ultimii ani, cele mai semnificative operațiuni din ultima vreme înregistrate au avut loc în preajma alegerilor prezidențiale americane din 2020, având în vedere precedentul alegerilor din 2016, vizate de operațiunile cibernetice ale Federației Ruse. Spre exemplu, operațiunea cibernetică Stuxnet a făcut parte dintr-o campanie mai largă a SUA, Israelului și statelor partenere de a priva Iranul de abilitatea de a produce uraniu îmbogățit (Kello 2017, p. 63).

Totuși, operațiunile cibernetice ofensive în spațiul cibernetic, indiferent de actorul statal care le desfășoară, lasă în urmă probleme pentru toți utilizatorii internetului. Serviciile de intelligence sunt printre cei mai importanți actori din spațiul cibernetic, în special cu privire la utilizarea strategică a acestuia. În afară de operațiunile cibernetice ofensive și defensive propriu-zise, serviciile de intelligence caută și exploatează breșe de securitate secrete în sistemele de operare și software-urile utilizate la scară largă pentru a obține accesul în diferite locații în cadrul infrastructurii de Internet. Implanturile și punctele de acces obținute de serviciile de intelligence pot fi utilizate pentru mai multe scopuri, precum spionaj sau acțiuni disruptive, iar acestea pot fi activate oricând atâta vreme cât victimele nu reușesc să depisteze vulnerabilitatea și intruziunile. Astfel, în ceea ce privește operațiunile cibernetice ofensive, actorii statali ajung să pună în pericol propria securitate națională prin identificarea și menținerea secretă a vulnerabilităților, atâta vreme cât acestea pot fi utilizate și de alți actori. (Dunn Cavelty și Egloff 2019, p. 47)

În plus, caracteristicile de bază ale democrației liberale, pluralismul politic, libertatea mediei, economia deschisă și statul de drept sunt văzute și exploatate ca vulnerabilități prin utilizarea interferențelor hibride. Respectând statul de drept și promovarea libertăților civile, democrațiile liberale au un set limitat de mijloace pentru a contracara amenințările cibernetice (inclusiv cele care vizează alegerile) și informaționale, la fel și în ceea ce privește limitarea

activităților partidelor extremiste sau a grupurilor de media cumpărate sau controlate de un alt actor și utilizate pentru interferențe hibride. Totuși, vulnerabilitățile democrațiilor liberale pot fi adresate tot prin utilizarea principiilor democrației liberale, chiar politica incluzivă și abilitatea de a gestiona schimbările reprezintă atuuri în combaterea interferențelor hibride. Spre exemplu, organizațiile neguvernamentale și mișcările sociale pot oferi mecanisme democratice și eficiente pentru monitorizarea și dezvăluirea interferențelor hibride, iar libertatea mediei reprezintă un avantaj major, funcționând tot ca un monitor al interferențelor, mai ales ținând cont de jurnalismul de investigație (ex. grupul *Bellingcat*) (Wigell 2019, pp. 268-273).

Statele trebuie să depună eforturi pentru a promova cultura rezilienței cibernetice prin promovarea igienei cibernetice și prin creșterea conștientizării la toate nivelurile societății și a guvernelor (Pawlak 2018, p. 113). Totuși, eforturile activităților și măsurilor din sfera apărării și securității cibernetice trebuie să reprezinte în primul rând responsabilitatea statului și a tuturor instituțiilor acestuia, a companiilor private din domeniile legate de tehnologie și operatorilor infrastructurilor critice, iar abia apoi responsabilitatea mediului economic, a mediei, a societății civile, a academiei sau a indivizilor.

Statele trebuie să integreze democrația și drepturile omului în eforturile legate de securitatea cibernetică pentru a se asigura că măsurile respectă libertățile online și drepturile omului, reprezentând o alternativă pentru autoritarismul digital (Yayboke și Brannen 2020, p. 7). Libertatea de exprimare și dreptul la intimitate trebuie să fie văzute ca chestiuni în favoarea sporirii securității, având în vedere că masa de date care va fi necriptată ar scădea, ceea ce ar reduce și criminalitatea cibernetică și spionajul cibernetic (Dunn Cavelty 2014, p. 711). Promovarea unui internet liber și sigur este esențială pentru oferirea unui model democratic de guvernare a Internetului și de asigurare a securității cibernetice care să reprezinte o alternativă pentru autoritarismul digital (Yayboke și Brannen 2020, p. 8).

Concluzii

Operațiunile cibernetice discutate în cadrul studiului au afectat în mod semnificativ statele vizate, iar multe dintre ele (precum WannaCry, NotPetya sau atacul împotriva rețelei electrice a Ucrainei) au reprezentat puncte de cotitură poate chiar mai mari față de atacurile cibernetice împotriva Estoniei din 2007. În plus, a fost evidențiat rolul Rusiei în campaniile cibernetice împotriva statelor euro-atlantice, operațiunile cibernetice fiind incluse în cadrul unor campanii hibride de influențare și subminare a statelor vizate. Totodată, un impact negativ asupra securității cibernetice la nivel global și a spațiului cibernetic l-au avut și operațiunile cibernetice ale Chinei, Coreei de Nord, Iranului, și inclusiv o parte din activitățile cibernetice

ofensive ale Statelor Unite și practicile agențiilor de intelligence. Cu toate acestea, statele euro-atlantice au depus eforturi de a-și consolida apărarea și securitatea cibernetică, ținând cont și de respectarea valorilor democratice, a drepturilor omului și a libertăților civile, în comparație cu modelul autoritarismului digital al Rusiei și Chinei. Mai mult, statele democratice trebuie să elaboreze și să adopte un model democratic pentru guvernarea Internetului pentru a putea combate autoritarismul digital.

Apărarea cibernetică în contextul războiului hibrid trebuie să fie integrată în cadrul unei campanii mai largi de apărare împotriva setului de mijloace al războiului hibrid, iar răspunsurile și măsurile luate în urma operațiunilor cibernetice trebuie să includă un set larg de măsuri, operațiunile cibernetice și apărarea cibernetică fiind centrale, dar nu și singurele măsuri. Totodată, incidentele cibernetice majore provocate de actori statali nu sunt aproape niciodată incidente izolate sau singulare, ci sunt integrate de statul respectiv în cadrul unei campanii cibernetice mai largi, dar și în cadrul unei campanii informaționale și a unei campanii de influență sau tentative de schimbare a comportamentului, atitudinii sau cursurilor de politică internă sau externă al statului vizat, și a mijloacelor războiului hibrid. Așadar, și apărarea cibernetică trebuie implementată în același mod și ținând cont de aceleași elemente.

În condițiile în care competiția dintre statele euro-atlantice și Rusia a fost intensificată în ultimii ani, la fel și cea cu China, este de așteptat ca operațiunile cibernetice să crească atât în număr, cât și în intensitate în următoarea perioadă, dar și ca Rusia să exploateze situația creată în urma războiului de agresiune împotriva Ucrainei pentru a lansa noi atacuri cibernetice distructive, în timp ce China își va continua, cel mai probabil, campaniile de spionaj cibernetic. Totodată, dezvoltarea continuă a Internetului și a mijloacelor digitale, digitalizarea continuă și extinderea spațiului cibernetic vor crea noi oportunități pentru operațiuni cibernetice, fiind foarte probabil ca în următoarea perioadă să iasă în evidență și rolul actorilor non-statali, inclusiv a celor sprijiniți de actori statali.

Spațiul cibernetic este afectat în mod direct de conflicte, mai ales de operațiunile cibernetice care vizează infrastructura critică și cele prin care se încearcă subminarea încrederii publice, devenind și din ce în ce mai dependent și interconectat cu tehnologiile spațiale, inteligența artificială (*Artificial Intelligence* – AI) și calculatoarele cuantice, extinzând spațiul cibernetic și legându-l de mai multe domenii de politici publice. În plus, AI-ul va deveni un element esențial al securității cibernetice, având un impact major atât pentru operațiunile ofensive, cât și pentru cele defensive. În acest context, dezvoltarea *Internet of Things* (Internetul Obiectelor) va reprezenta o provocare majoră pentru securitatea cibernetică, odată

cu interconectarea la Internet a aparatelor electrocasnice, a sistemelor de sănătate sau a mașinilor. (Dunn Cavelty și Wenger 2020, p. 23; Healey 2019, p. 2; Willett 2021, p. 19)

Bibliografie

Balzacq, Thierry, și Myriam Dunn Cavelty. 2016. „A theory of actor-network for cyber-security". *European Journal of International Security* 1, nr. 2: 176-198.

Barrinha, André, și Thomas Renard. 2020. „Power and diplomacy in the post-liberal cyberspace". *International Affairs* 96, nr. 3: 749-766.

Buchanan, Ben. 2016. *The Cybersecurity Dilemma. Hacking, Trust, and Fear Between Nations*. New York: Oxford University Press.

Burton, Joe, și Clare Lain. 2020. „Desecuritising cybersecurity: towards a societal approach". *Journal of Cyber Policy* 5, nr. 3: pp. 449-470.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

Dunn Cavelty, Myriam, și Andreas Wenger. 2020. „Cyber security meets security politics: Complex technology, fragmented politics, and networked science". *Contemporary Security Policy* 41, nr. 1: 5-32.

Dunn Cavelty, Myriam, și Andreas Wenger. 2022. *Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation*. Londra și New York: Routledge.

Dunn Cavelty, Myriam, și Florian J. Egloff. 2019. „The politics of cybersecurity: Balancing different roles of the state". *St. Antony's International Review* 15, nr. 1: pp. 37-57.

Dunn Cavelty, Myriam. 2014. „Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities". *Science and engineering ethics* 20, nr. 3: 701-715.

Happa, Jassim, și Graham Fairclough. 2017. „A Model to Facilitate Discussions About Cyber Attacks". În *Ethics and Policies for Cyber Operations*, ed. Mariarosaria Taddeo și Ludovica Glorioso, pp. 169-186. Cham: Springer.

Healey, Jason. 2019. „The implications of persistent (and permanent) engagement in cyberspace". *Journal of Cybersecurity* 5, nr. 1:1-15.

Hoffman, Frank G. 2007. *Conflict in the 21st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies.

Hoffman, Frank G. 2009. „*Hybrid threats: Reconceptualizing the evolving character of modern conflict"*. *Strategic Forum*, nr. 240: pp. 1-8.

Isnarti, Rika. 2016. „A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War". *Andalas Journal of International Studies (AJIS)* 5, nr. 2: pp. 151-165.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven și Londra: Yale University Press.

Kello, Lucas. 2018. „Cyber Defence". În *The Handbook of European Defence Policies and Armed Forces*, ed. Hugo Meijer și Marco Wyss, pp. 659-672. Oxford: Oxford University Press.

Kello, Lucas. 2021. „Cyber legalism: why it fails and what to do about it". *Journal of Cybersecurity* 7, nr. 1: 1-15.

Lasconjarias, Guillaume, și Jeffrey Arthur Larsen. 2015. *NATO's Response to Hybrid Threats*. Roma: NATO Defense College.

Lewis, James A. 2015. „Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine". În *Cyber War in Perspective: Russian Aggression against Ukraine*, editat de Kennet Geers, pp. 39-48. Tallinn: NATO CCD COE Publications.

Limnell, Jarno. 2018. „Russian activities in the EU". În *Hacks, leaks and disruptions: Russian cyber strategies*, ed. Nicu Popescu și Stanislav Secrieru, pp. 65-74. *Chaillot Paper* 148. Paris: EU Institute for Security Studies.

Microsoft. 2022. „Defending Ukraine: Early Lessons from the Cyber War". *Microsoft*, 22 iunie. Disponibil la: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Nye, Joseph S. 2018. „Normative Restraints on Cyber Conflict". *Belfer Center for Science and International Affairs*, august 2018. Disponibil la: https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf.

Pawlak, Patryk. 2018. „Protecting and defending Europe's Cyberspace". În *Hacks, leaks and disruptions: Russian cyber strategies*, ed. Nicu Popescu și Stanislav Secrieru, pp. 103-114. *Chaillot Paper* 148. Paris: EU Institute for Security Studies.

Polyakova, Alina, și Chris Meserole. 2019. „Exporting digital authoritarianism. The Russian and Chinese models". *Brookings*, august 2019. Disponibil la: https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Polyakova, Alina, și Spencer P. Boyer. 2018. „The future of political warfare: Russia, the West, and the coming age of global digital competition". *Brookings*, martie 2018. Disponibil la: https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/.

Rinelli, Sebastian, și Isabelle Duyvesteyn. 2018. „The Missing Link: Civil-Military Cooperation and Hybrid Wars". În *A Civil-Military Response to Hybrid Threats*, ed. Eugenio Cusumano și Marian Corbe, pp. 17-40. Cham: Springer.

Rõigas, Henry. 2017. „Cyber War in Perspective: Lessons from the Conflict in Ukraine". În *A Civil-Military Response to Hybrid Threats*, ed. Eugenio Cusumano și Marian Corbe, pp. 233-258. Cham: Springer.

Slayton, Rebecca. 2017. „What is the cyber offense-defense balance? Conceptions, causes, and assessment". *International Security* 41, nr. 3: pp. 72-109.

Steiger, Stefan, Sebastian Harnisch, Kerstin Zettl, și Johannes Lohmann. 2018. „Conceptualising conflicts in cyberspace". *Journal of Cyber Policy* 3, nr. 1: pp. 77-95.

Wigell, Mikael. 2019. „Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy". *International Affairs* 95, nr. 2: 255-275.

Willet, Marcus. 2021. „Lessons of the SolarWinds Hack". *Survival* 63, nr. 2: 7-26.

Yayboke, Erol, și Sam Brannen. 2020. „Promote and Build. A Strategic Approach to Digital Authoritarianism". *CSIS Briefs*, 15 octombrie. Disponibil la: https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism.