CZU: 004.056 DOI: 10.46727/c.steam-2023.p349-356

STUDIUL AMENINŢĂRILOR CIBERNETICE ÎN DOMENIUL MILITAR

Fiodor TIMERCAN, lector universitar
Academia Militară „Alexandru cel Bun”

Abstract. Pornind de la acceptarea generală, definirea ameninţării de origine politico-militară necesită unele clarificări. Fie că se referă la încălcarea drepturilor fundamentale ale statelor sau la sistemele de securitate a percepției transpunerii obiectivelor amenințării rămase în fapte, încadrându-se printre pericolele virtuale. Ele declanșează întotdeauna reacțiile necesare pentru a contracara efectele amenințării. Situația devine gravă atunci când sunt supradimensionate. Poate fi inițiată sau o reacție în lanț, greu de controlat, în care binomul newtonian „acțiune-reacție” se poate înmulți până la distrugerea sistemului care a generat-o.
Această atitudine poate fi generată mai des de amenințări asimetrice, concept care este folosit destul de des în literatura de specialitate actuală. Ea semnifică „amenințarea care rezultă din posibilitatea de a folosi mijloace sau metode diferite pentru a lovi sau neutraliza punctele forte ale unui adversar prin exploatarea slăbiciunilor acestuia pentru a obține un rezultat disproporționat.
Cuvinte cheie: amenințări cibernetice, atacuri cibernetice, securitate cibernetică, spațiu cibernetic.

Abstract. Starting from the general acceptance, the definition of the threat of politico-military origin requires some clarification. Whether it refers to the infringement of the fundamental rights of the states or the security systems of the perception of the transposition of the objectives of the remaining threat into facts, falling among the virtual dangers. They always trigger the reactions necessary to counteract the effects of the threat. The situation becomes serious when they are oversized. It can be initiated or a chain reaction, difficult to control, in which the Newtonian binomial "action-reaction" can multiply until the destruction of the system that generated it.
This attitude can be more often generated by asymmetric threats, a concept that is used quite often in the current specialized literature. It signifies "the threat resulting from the possibility of using means or different methods to strike or neutralize the strengths of an adversary by exploiting his weaknesses in order to obtain a disproportionate result.
Keywords: cyber threats, cyber attacks, cyber security, cyber space.

Introducere

Pe măsură ce armatele ţărilor dezvoltate exploatează avantajele oferite de spaţiul virtual, infrastructura acestora devine tot mai vulnerabilă atacurilor cibernetice. Fenomenul agresiunilor a cunoscut o diversificare permanentă, direct proporţională cu dezvoltarea tehnologiilor informaţiei şi a societăţii informaţionale. Metodele de atac sunt permanent adaptate evoluţiei din domeniul tehnologic şi vulnerabilităţilor identificate. Teoreticienii consideră spaţiul cibernetic drept al cincilea domeniu în care se poate desfăşura un război, după sol, mare, aer şi spaţiu, caracterizat prin dinamism extrem, asimetrie, predictibilitate redusă şi dificultatea atribuirii agresiunilor.

În cazul armei-cheie a secolului al XX-lea, bomba nucleară, ţările ce o puteau folosi în luptă au ales să nu o facă, fiind descurajate de faptul că un contraatac ar fi fost la fel de

devastator. În schimb, atacul cibernetic ar putea evita acest impediment dacă victima atacului nu ştie împotriva cărei ţări să lanseze contraatacul.

Primul atac cibernetic a fost semnalat în 1982, când spionii sovietici au furat un sistem de control computerizat de la o companie canadiană, fără să ştie că specialiştii CIA reuşiseră să introducă în software-ul acestuia o linie de cod care a generat o explozie masivă la o conductă de gaz din Siberia. Deflagraţia a fost atât de mare încât a fost detectată din spaţiu de sateliţii americani, iar Thomas Reed, fost comandant al aviaţiei SUA, a descris-o în autobiografia sa ca fiind „cea mai mare explozie non-nucleară detectată vreodată din spaţiu".

Cu toate acestea, atacurile cibernetice au intrat în atenţia opiniei publice abia după 25 de ani de la acest eveniment, respectiv în 2007, când o ţară întreagă - Estonia - a fost afectată, ministerele, băncile şi numeroase companii fiind nevoite să îşi oprească activitatea. Primul atac cibernetic asupra unei întregi ţări a venit pe fondul unei dispute politice pe tema mutării unui monument dedicat eroilor sovietici, propunere îndelung contestată de minoritatea rusă din Estonia şi de Kremlin. Majoritatea informaţiilor au indicat ca sursă a atacului adrese de internet originare din Rusia.

Un an mai târziu, în 2008, Georgia a suferit atacuri similare, într-o perioadă ce a coincis cu conflictul georgiano-rus din Osetia de Sud. Din cauza atacurilor venite dinspre Rusia, router-ele din Turcia şi Rusia ce făceau legătura cu Georgia au fost supraîncărcate cu date despre ţara gruzină, astfel că traficul în exterior a fost complet sufocat, cetăţenii Georgiei fiind în imposibilitatea de a accesa vreun site. De asemenea, Georgia a pierdut controlul asupra domeniului ".ge", fiind nevoită să transfere site-urile guvernamentale pe servere din afara ţării.

Atacurile cibernetice asupra celor două ţări au determinat o reevaluare a doctrinelor militare ale statelor dezvoltate, securitatea cibernetică căpătând astfel mai multă importanţă.

Totuşi adevăratul început al războiului cibernetic poate fi datat în anul 2010, odată cu apariţia primei arme cibernetice (virusul Stuxnet), primul virus proiectat să preia sub control şi să saboteze subtil infrastructurile critice ale unui stat. În 2011, a fost descoperit Duqu, un troian cu caracteristici similare Stuxnet, dar proiectat să acţioneze ca un „backdoor" în sistemul infectat şi să fure informaţii confidenţiale. Anii următori s-au remarcat prin descoperirea unui număr tot mai mare de agresiuni cibernetice persistente (de tip Advanced Persistent Threat), cu impact semnificativ asupra securităţii naţionale.

Amintim întregul arsenal de arme cibernetice descoperit: Flame (apreciat de specialiştii în domeniu drept cel mai sofisticat malware cunoscut până în prezent), Wiper, Mahdi, Shamoon, Gauss - malware produse de actori statali antagonici, folosite împotriva unor infrastructuri critice (transport resurse energetice, bănci, agenţii guvernamentale, universităţi). Aceste descoperiri subliniază faptul că securitatea naţională nu este aşa de

sigură pe cât se credea. Războiul cibernetic a adăugat o nouă dimensiune, prezentând lumii, în mod clar, modul în care ţările avansate din punct de vedere tehnologic îşi pot utiliza cunoştinţele superioare pentru a ataca alte ţări.

Progresul atacurilor cibernetice în profil militar

Spaţiul cibernetic răspândit la scară globală, o invenţie veche de câteva decenii, a evoluat. Dar la fel au făcut şi ameninţările. Viermii şi viruşii s-au transformat din simple mici probleme agasante în serioase provocări de securitate şi instrumente perfecte ale spionajului cibernetic.

Atacurile executate cu implicarea unui grup numeros de calculatoare care generează refuzul de a presta serviciile solicitate (distributed denial of service – DDOS), privite până acum ca, de fapt, nimic mai mult decât nişte „blocaje de protest", au devenit un instrument în războiul informaţional.

Şi, în fine, în iunie 2010, softul maliţios „Stuxnet" a devenit public, ceva ca o „bombă de penetrare a ţintelor blindate digitală" care a atacat programul nuclear iranian. Prin acesta, avertizările timpurii transmise de experţi începând din 2001 au devenit realitate, sugerând că dimensiunea cibernetică ar putea să fie folosită mai devreme sau mai târziu pentru executarea unor atacuri serioase care vor avea consecinţe letale în lumea reală.

Pe timpul crizei generate de Kosovo, NATO s-a confruntat cu primele sale incidente serioase cauzate de atacuri cibernetice. Acest lucru a făcut ca, printre altele, contul e-mail al NATO să fie blocat timp de câteva zile pentru vizitatorii externi şi ca funcţionarea website-ului Alianţei să fie întreruptă în mod repetat.

Într-un mod tipic pentru acea perioadă, s-a considerat, totuşi, că dimensiunea cibernetică a conflictului nu a făcut altceva decât să limiteze acţiunile întreprinse în cadrul campanei de informare a NATO. Atacurile cibernetice erau privite ca un risc, dar ca unul limitat ca amploare şi potenţial distructiv, solicitând doar răspunsuri tehnice limitate, acompaniate de eforturi de informare a publicului la o scară mică.

A fost nevoie să se producă evenimentele din 11 septembrie pentru ca acea percepţie să se schimbe. Şi a mai fost nevoie să se producă incidentele din Estonia din primăvara lui 2007 pentru a se putea beneficia de întreaga atenţie politică în privinţa acestei surse crescânde de ameninţări la adresa siguranţei publice şi stabilităţii statelor. Un val masiv de atacuri cibernetice de trei săptămâni a demonstrat că ţările membre NATO, puternic dependente de comunicaţiile electronice, au fost extrem de vulnerabile pe frontul cibernetic.

Conştientizarea crescândă a seriozităţii ameninţării cibernetice a fost accentuată şi mai mult de incidentele din anii care au urmat. În 2008, unul dintre cele mai serioase atacuri de până în prezent a fost lansat împotriva sistemului american de computere. Prin

intermediul unui singur memory stick conectat la un laptop al armatei, la o bază militară din Orientul Mijlociu, un program spion s-a răspândit nedetectat, atât în sistemele clasificate, cât şi în cele neclasificate. Acest eveniment a realizat ceea ce a echivalat cu un cap de pod digital, prin care mii de dosare cu date au fost transferate în servere aflate sub control străin.

Începând de atunci, spionajul cibernetic a devenit o ameninţare aproape constantă. Incidente similare s-au produs în aproape toate statele membre NATO şi – mai important – recent, din nou, în Statele Unite. De această dată, au fost afectate mai mult de 72 de companii, inclusiv 22 de birouri guvernamentale şi 13 contractori din domeniul apărării.

Aceste incidente numeroase petrecute în ultimii cinci sau şase ani echivalează cu un transfer fără precedent în istorie de resurse valoroase şi secrete naţionale strict păzite către un destinatar anonim şi cel mai probabil rău intenţionat şi ele demonstrează clar două lucruri:

- Până în prezent, cei mai periculoşi actori în domeniul cibernetic sunt tot statele-naţiuni. În pofida unor capabilităţi ofensive aflate din ce în ce mai mult la dispoziţia reţelelor militare care ar putea să fie folosite în viitor, de asemenea, de actori non-statali precum teroriştii, spionajul şi sabotajul de înaltă sofisticare în domeniul cibernetic au în continuare nevoie de capabilităţile, hotărârea şi raţiunea cost-beneficii ale unui stat-naţiune.

- Pagubele fizice devastatoare şi terorismul cibernetic cinetic real nu s-au produs încă. Dar este clar că tehnologia atacurilor evoluează de la mici probleme agasante la o ameninţare serioasă la adresa securităţii informaţiilor şi chiar la adresa infrastructurii naţionale de o importanţă crucială.

Nu există nici o îndoială că unele ţări investesc deja masiv în capabilităţi cibernetice care pot fi folosite în scopuri militare. La prima privire, cursa digitală a înarmării se bazează pe o logică clară şi implacabilă, deoarece domeniul războiului cibernetic oferă numeroase avantaje: este asimetric, atrăgător prin costurile scăzute şi atacatorul deţine iniţial toate avantajele.

Mai mult decât atât, nu există practic nici o formă reală de descurajare în cadrul războiului cibernetic, deoarece până şi identificarea atacatorului este extrem de dificilă şi, respectând dreptul internaţional, probabil, aproape imposibilă. În aceste condiţii, orice formă de retorsiune militară ar foarte problematică, atât din punct de vedere legal, cât şi din punct de vedere politic.

Provocări şi ameninţări cibernetice

Evoluţiile în planul securităţii globale atestă revenirea la politica de forţă, a ameninţărilor şi intervenţiilor militare asupra unor state independente şi suverane. Instrumentul militar continuă să rămână un mijloc de extindere a influenţei, de apărare a

intereselor naţionale şi de promovare a obiectivelor de politică externă. Cumulul de factori ce compun un mediu de securitate complex şi extrem de dinamic impune aplicarea de măsuri pe mai multe planuri, în care cel militar redobândește relevanţă.

Statele lumii se află în faţa unor provocări majore, cu implicaţii greu de prevăzut asupra securităţii sale. Pe de o parte, este necesară identificarea unei soluţii coerente în faţa ameninţărilor de natură hibridă. Atacurile cibernetice sunt o categorie complexă de ameninţări, prin dinamica accentuată, caracterul global, dificultatea identificării sursei atacului şi a stabilirii măsurilor eficiente de contracarare. Ţintele probabile ale acestor atacuri pot fi atât obiectivele de infrastructură critică civilă, cât şi sistemele de comunicaţii şi tehnologiile informatice din domeniul apărării.

Ameninţările specifice spaţiului cibernetic se caracterizează prin asimetrie şi dinamică accentuată şi caracter global, ceea ce le face dificil de identificat şi de contracarat prin măsuri proporţionale cu impactul materializării riscurilor.

Ţările lumii se confruntă în prezent cu ameninţări provenite din spaţiul cibernetic la adresa infrastructurilor critice, având în vedere interdependenţa din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri precum cele din sectoarele financiar bancar, transport, energie şi apărare naţională. Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeaşi măsură atât sectorul privat, cât şi cel public.

Ameninţările la adresa spaţiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate pe factorii motivaţionali şi impactul asupra societăţii. În acest sens, putem avea în vedere criminalitatea cibernetică, terorismul cibernetic şi războiul cibernetic, având ca sursă atât actori statali, cât şi non-statali. Ameninţările din spaţiul cibernetic se materializează – prin exploatarea vulnerabilităţilor natură umană, tehnică şi procedurală – cel mai adesea în atacuri cibernetice împotriva infrastructurilor care susţin funcţii de utilitate publică ori servicii ale societăţii informaţionale a căror întrerupere / afectare ar putea constitui un pericol la adresa securităţii naţionale, accesarea neautorizată a infrastructurilor cibernetice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice ori restricţionarea ilegală a accesului la aceste date, spionajul cibernetic, cauzarea unui prejudiciu patrimonial, hărţuirea şi şantajul persoanelor fizice şi juridice, de drept public şi privat.

Folosirea noilor tehnologii şi a spaţiului cibernetic pentru derularea de atacuri constituie atât o modalitate de a pune în practică un nou tip de ameninţare – cibernetică – dar şi o modalitate de a controla alte ameninţări de tip hibrid, precum lupta în plan informaţional.

Spaţiul cibernetic reprezintă un mediu care oferă atacatorului posibilitatea de a acţiona în anonimitate – disimulând atacul, locul de origine şi identitatea atacatorului – şi

folosind resurse financiare, materiale şi umane reduse în comparaţie cu o acţiune militară clasică.

Intensitatea şi complexitatea tehnologică a acestor atacuri (de regulă atacuri de tip Advanced Persistent Threat – APT -), ţintele strategice vizate, rezultatele obţinute (în termeni de filtrare de informaţii strategice, de dezinformare şi chiar de distrugere a serviciilor) şi, nu în ultimul rând, motivaţia atacatorilor (care este politică prin natura sa, şi nu infracţională) atenţionează asupra apartenenţei lor la arsenalul ameninţărilor de tip hibrid. Delimitarea faţă de atacurile aparținând criminalităţii cibernetice este clară.

Astfel de atacuri sunt realizate de state, dar pot deveni şi apanajul altor categorii de actori, non-statali, precum organizaţii teroriste, pe măsură ce ar dispune de capabilităţile tehnologice şi resursele financiare necesare derulării unor atacuri cibernetice de complexitate ridicată. Atacurile cibernetice reprezintă aşadar una dintre cele mai noi ameninţări hibride, care câştigă din ce în ce mai multă publicitate în ultimii ani.

Atacurile din 2015 asupra unor infrastructuri din domeniul energetic din Ucraina, care au determinat întreruperea furnizării de energie electrică, paralizând industria locală şi afectând totodată populaţia civilă, sunt considerate un exemplu de folosire a atacurilor cibernetice ca parte a războiului hibrid, având în vedere că au însoţit un conflict militar şi au cauzat pagube substanţiale unei infrastructuri critice.

Anihilarea ameninţărilor cibernetice militare

Pregătirea unui răspuns eficient în faţa ameninţărilor cibernetice, ca parte a ameninţărilor hibride, necesită dialog şi cooperare atât la nivel politic şi operaţional, atât la nivelul statelor afectate, între instituţiile cu responsabilităţi în asigurarea securităţii cibernetice, cât şi în format regional şi internaţional. Măsurile şi acţiunile întreprinse trebuie să aibă în vedere consolidarea gradului de conştientizare a ameninţării şi creşterea rezilienţei societăţii, infrastructurilor şi instituţiilor prin identificarea celor mai bune forme de protecţie.

Pentru a creşte reziliența în faţa ameninţării cibernetice este important să fie înţeleasă natura ameninţării, să fie cunoscute şi asumate vulnerabilităţile pe care un adversar le-ar putea exploata. Fiecare stat trebuie să conştientizeze că nu poate asigura securitatea cibernetică fără consolidarea capacităţilor de cooperare şi coordonare în culegerea şi schimbul de informaţii, precum şi identificarea şi evaluarea riscurilor şi vulnerabilităţilor.

De asemenea, în asigurarea rezilienţei în faţa ameninţării cibernetice un rol important îl are existenţa capacităţii de a face faţă ameninţării, de a se adapta şi transforma, prin dezvoltarea unor capabilităţi de avertizare timpurie şi răspuns şi prin promovarea şi dezvoltarea unei culturi de securitate cibernetică.

Crearea şi dezvoltarea unei culturi de securitate cibernetică, atât la nivelul societăţii civile, cât şi la nivelul decidenţilor politici şi instituţiilor publice, prin derularea de parteneriate public-private, programe educaţionale, exerciţii comune, conferinţe, seminarii, dezbateri şi prezentări publice pe tema ameninţării cibernetice, ca parte a ameninţărilor de tip hibrid.

Aşadar, asigurarea securităţii cibernetice în faţa unei ameninţări care nu cunoaşte frontiere şi care poate viza atât entităţi publice, cât şi private, trebuie să reprezinte o preocupare constantă nu doar pentru guverne, dar şi pentru entităţile private şi pentru cetăţeni. Aceste entităţi trebuie să coopereze în prevenirea şi combaterea atacurilor cibernetice care devin din ce în ce mai numeroase şi mai sofisticate, provocând prejudicii importante în lumea reală. În final, trebuie să avem în vedere că, indiferent de modul de manifestare al unui viitor conflict, atacurile cibernetice vor fi parte integrantă a acestuia.

Crearea Sistemului Naţional de Securitate Cibernetică – SNSC care să reprezinte cadrul de cooperare care reuneşte autorităţi şi instituţii publice, mediul academic şi cel de afaceri, asociaţii profesionale, organizaţii neguvernamentale, cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor pentru asigurarea securităţii componentei naţionale a spaţiului cibernetic. Coordonarea activităţii Sistemului Naţional de Securitate Cibernetică trebuie asigurată de un comitet, având ca obiective implementarea Programului Naţional în domeniu, managementul acţiunilor, la nivel naţional, în cazul unui atac cibernetic, respective corelarea demersurilor instituţiilor componente în cadrul formatelor de cooperare internaţională. Sistemul Naţional de Securitate Cibernetică trebuie să asigure cunoaşterea, prevenirea şi contracararea unui atac împotriva componentei naţionale a spaţiului cibernetic, inclusive managementul consecinţelor.

Componenta de cunoaştere trebuie să asigure informaţiile necesare în elaborarea măsurilor pentru prevenirea efectelor unor incidente cibernetice. Componenta de prevenire va fi principalul mijloc de asigurare a securităţii cibernetice. Acţiunile preventive reprezintă cea mai eficientă modalitate atât de a reduce extinderea pe teritoriul unei ţări a mijloacelor specifice unui atac cibernetic, cât şi de a limita efectele utilizării acestora.

Componenta de contracarare trebuie să asigure o reacţie eficientă la atacuri cibernetice, prin identificarea şi blocarea acţiunilor ostile în spaţiul cibernetic, menţinerea sau restabilirea disponibilităţii infrastructurilor cibernetice vizate şi identificarea şi sancţionarea potrivit legii a autorilor. Succesul activităţilor desfăşurate depinde în mod esenţial de cooperarea, inclusiv în formule de parteneriat public privat, între deţinătorii infrastructurilor cibernetice şi autorităţile statului abilitate să întreprindă măsuri de prevenire, contracarare, investigare şi eliminare a efectelor unei ameninţări materializate printr-un atac.

Concluzii

Niciodată în istoria modernă a omenirii nu au existat atâtea elemente de incertitudine. În ciuda numeroaselor ipoteze emise în anii din urmă, puţini sunt capabili să întrevadă ce se va întâmpla pe termen mediu sau lung, iar ipotezele lor să fie veridice. Valorile în creştere ale componentelor noii ecuaţii de securitate conduc la concluzia că am intrat într-o epocă a insecurităţii strategice. Situaţia este cu atât mai complicată cu cât procesul globalizării continuă, ceea ce înseamnă că nimeni nu se poate considera în afara jocului. Nevoia de autoprotecţie a unor state ar putea să provoace un al treilea reflux al democratizării, care să pună capăt celui de-al treilea flux al democratizării. Care sunt statele cele mai ameninţate nu este greu de ghicit, dar nici democraţiile consolidate şi marile puteri nu se pot considera la adăpost.

Din această perspectivă noile ameninţări la adresa securităţii obligă statele să lucreze împreună pentru apărarea valorilor comune de democraţie, securitate şi libertate.

Drumul din faţa noastră nu este uşor. Pentru a dace faţă provocărilor secolului al XXI-lea este nevoie de voinţă politică, cât şi de eforturi financiare şi militare semnificative din partea tuturor. Mai mult, este nevoie de cooperare şi solidaritate din partea tuturor membrilor comunităţii pentru protejarea valorilor comune.

Bibliografie

1. Ameninţări la adresa securităţii. Editura Universităţii Naţionale de Apărare Bucureşti, 2004, 6, 22, 23 p.
2. ENISA Threat Landscape, ediţie online.
3. http://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/ accesat la data de 09 octombrie 2023, ora 10.16.
4. https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm accesat la data de 10 octombrie 2023, ora 09.30.
5. ЗАВАЛЬСКИЙ, И. Кибервойна: угрозы и защита, Сборник докладов 7-го симпозиума по вопросам безопасности Черноморского и Каспийского регионов, Одесса.
6. http://www.descopera.ro/capcanele-nternetului/9627768-traim-in-epoca-ciber-razboaielor accesat la data de 11 octombrie 2023, ora 12.28.;
7. https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index. accesat la data de 11 octombrie 2023, ora 15.45.;