INFLUENȚA DIMENSIUNII CIBERNETICE ASUPRA ACTIVITĂȚII FORȚELOR AERIENE STUDIU DE CAZ: CONFLICTUL DIN UCRAINA

Drd. Vasile-Cristian ONESIMIUC
Universitatea Națională de Apărare „Carol I”, București
10.55535/GMR.2023.4.10

Dimensiunea cibernetică a jucat un rol important în timpul conflictului din Ucraina, dar activitățile cibernetice nu au avut intensitatea prognozată de mulți experți militari. Cu toate acestea, este evident că această dimensiune este foarte utilizată de ambele părți ale conflictului și, în plus, această dimensiune a fost activă nu numai pe toată durata conflictului început în 2014, ci și înainte de anexarea Peninsulei Crimeea. Creșterea unor astfel de activități înainte de începerea invaziei din 2022 nu a făcut altceva decât să sublinieze importanța domeniului cibernetic pentru viitoarele conflicte, securitatea forțelor aeriene fiind o provocare continuă, având în vedere că aceste forțe sunt printre primele care au fost utilizate în conflict, atât din partea Rusiei, cât și a Ucrainei.

Conflictul din Ucraina a arătat, încă o dată, că dimensiunea cibernetică este și trebuie luată în considerare în fiecare etapă, pentru a asigura securitatea națională, înainte, în timpul și după conflictul convențional, dar nu trebuie supraestimată în privința efectelor dorite și a celor care pot fi atinse.

Cuvinte-cheie: operații cibernetice, conflict convențional, forțe aeriene, securitate, capabilități.

INTRODUCERE

Conflictul început în februarie 2022 a confirmat faptul că forțele aeriene sunt printre primele forțe utilizate pentru executarea de misiuni de luptă împotriva adversarului. De regulă, forțele aeriene sunt vârful de lance utilizat pentru proiectarea puterii militare a unui stat, mai ales în cazul acelor state care posedă forțe aeriene puternice. Forțele aeriene au reprezentat și continuă să reprezinte prima opțiune cu vizibilitate și impact imediat în ceea ce privește implicarea forțelor militare în cazul unor conflicte militare sau premergător acestora, pentru a determina adversarul să urmeze un anumit curs de acțiune sau să se abțină de la a executa anumite acțiuni ostile. Evaluările inițiale din anul 2022 efectuate de către experții militari din numeroase state prevedeau o înfrângere rapidă a forțelor ucrainene. Din punct de vedere al mărimii forțelor, exista o inegalitate majoră în termen de cantitate și calitate a materialului militar deținut de cele două state aflate în conflict. Astfel, evaluările care dădeau credit total Rusiei în ceea ce privește obținerea foarte rapidă a victoriei prevalau, extrem de puțini fiind cei care îndrăzneau să creadă în continuare în ceea ce privește posibilitatea ca Ucraina să mai reziste tăvălugului rus măcar pentru o perioadă mai mare de două săptămâni. Promovarea extrem de puternică și de persistentă a forțelor armate ruse a condus la apariția, în mentalul colectiv, a sentimentului inutilității rezistenței ucrainene, coloanele nesfârșite de tehnică militară rusă din primele zile ale conflictului întărind această idee.

Dacă, din punct de vedere al puterii aeriene convenționale, lucrurile păreau relativ clare, în sensul că statele care dețin forțe aeriene moderne, cu aeronave de ultimă generație, pot să imprime o anumită conduită statelor care nu dețin forțe aeriene suficient de dezvoltate din punct de vedere al numărului și al calității aeronavelor de luptă, în ceea ce privește dimensiunea cibernetică a operațiilor aeriene lucrurile nu mai sunt atât de clare. Se impune, astfel, un demers științific care să abordeze acest subiect, în vederea identificării metodelor de optimizare a asigurării securității cibernetice pentru activitățile forțelor aeriene.

Din acest punct de vedere, cercetarea urmărește să răspundă la întrebarea dacă domeniul cibernetic este important și de actualitate pentru activitatea forțelor aeriene, având în vedere evoluțiile înregistrate în cadrul conflictului din Ucraina. În acest sens, scopul articolului este de a identifica, pe baza informațiilor din sursele

deschise disponibile, cum a fost integrat domeniul cibernetic în cadrul activității forțelor aeriene, în baza evaluărilor care au fost efectuate înainte de conflictul din Ucraina și care au fost elementele identificate pe timpul conflictului. Întrebările de la care s-au pornit în cadrul acestui demers au fost:

- Viitoarele conflicte vor avea o dimensiune cibernetică? Cât de mult va conta această dimensiune în cadrul activităților curente executate?
- Cum ar trebui integrată această dimensiune cibernetică în cadrul etapelor desfășurării conflictului?
- Integrarea dimensiunii cibernetice trebuie privită din perspectiva asigurării securității cibernetice în ansamblu sau trebuie să fie centrată pe asigurarea misiunii din punct de vedere cibernetic?

TRANZIȚIA DE LA SECURITATE CIBERNETICĂ DE ANSAMBLU LA ASIGURAREA MISIUNII

Spre deosebire de alte state dezvoltate din punct de vedere cibernetic, Rusia nu a fost atât de dornică de publicitate în ceea ce privește acțiunile executate, de regulă executând activități cibernetice în mod cât mai ascuns posibil (Caimeanu, 2021), pentru a nu lăsa urme sau a dezvălui interesul pentru anumite obiective care sunt vizate. Cu toate acestea, atacurile cibernetice nu sunt atât de anonime pe cât se poate crede, astfel că a fost posibilă identificarea unor legături ruse în atacurile cibernetice executate chiar și asupra unor state aparținând NATO sau non-NATO, așa cum a fost cazul Estoniei, în 2007, Georgiei, în anul 2008, Ucrainei, începând cu anul 2014, Muntenegru, în 2016, Franței, în anul 2017, ca să menționăm o parte din cele care au fost identificate.

Comandamentul cibernetic al SUA (USCYBERCOM) afirma, încă din anul 2018, că acțiunile cibernetice executate de către adversari se desfășoară sub pragul conflictelor armate, pentru a slăbi instituțiile statului și a prelua inițiativa la nivel strategic (https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM).

Autoritățile ucrainene se pare că au luat foarte în serios cele afirmate de către forțele militare americane, iar consecința directă a fost faptul că desfășurarea ulterioară a ostilităților în spațiul cibernetic nu a condus la obținerea rezultatelor dorite de către Rusia. De exemplu, atacul din anul 2015 din Ucraina, atribuit hackerilor ruși, împotriva rețelei de energie, atac care a afectat inclusiv facilități de transport aerian, a fost repetat și în anul 2016, dar cu efecte mai puțin intense decât la precedentul atac (Timea, Skopik, 2018, p. 43). Din punctul de vedere al Federației

Sursa: Command-Vision-for-USCYBERCOM-23-Mar-18

Ruse, forțele armate ruse se află în două stări, de război sau de pregătire pentru război, iar ambițiile politice ale conducătorilor au primit ca sprijin noi modalități de ducere a războiului fără a declara acest lucru în mod oficial, instrumentele reprezentate de atacurile cibernetice fiind privite drept elemente centrale pentru ducerea și câștigarea conflictelor contemporane (Lilly, 2022, p. 17).

Influența dimensiunii cibernetice asupra activității forțelor aeriene nu poate fi negată, chiar dacă este dificil de contabilizat. Din punctul acesta de vedere, lipsa contabilizării acțiunilor cibernetice poate conduce la o înțelegere redusă a domeniului cibernetic, atât a efectelor dorite, cât și a celor care pot fi obținute, nu numai din perspectiva atacatorului, ci și din cea a celui care se apără.

Problema cel mai dificil de rezolvat în ceea ce privește dimensiunea cibernetică este abundența de provocări existente. Chiar dacă sunt realizate progrese în anumite sectoare, acestea sunt rapid analizate de către adversar pentru a se prevala avantajul ofensivei asupra defensivei. În raportul citat, experții au estimat că grupările cibernetice ruse au evaluat rezultatul activităților cibernetice executate și au realizat ajustări ale armelor cibernetice pentru a obține efectele dorite.

Una dintre cele mai mari provocări din domeniul cibernetic în ceea ce privește operațiile aeriene este persistența campaniilor cibernetice executate de către un adversar puternic și extrem de dezvoltat în ceea ce privește arsenalul cibernetic. Aceste campanii cibernetice care nu au efecte imediate foarte vizibile trec oarecum pe sub radarul entităților care au ca obiect de activitate asigurarea apărării cibernetice, dar, în timp, această activitate aparent inofensivă poate să erodeze în mod semnificativ nu doar punctual forțele aeriene, ci poate avea efecte generalizate.

Războiul din Ucraina a arătat că un adversar nu a reușit să utilizeze dimensiunea cibernetică pentru a organiza desfășurarea de atacuri cibernetice de amploare

care să ducă la neutralizarea forțelor aeriene de așa natură încât acestea să nu mai fie în măsură să reacționeze la atacul convențional. Ce a fost observat este că atacurile cibernetice nu au fost nici devastatoare, nici suficiente pentru a neutraliza forțele adversarului, astfel că a devenit evident că este necesar să se intervină conjugat, atât cibernetic, cât și clasic, cu atacuri convenționale.

Conflictul din Ucraina nu a fost, în această privință, similar cu acțiunea Israelului din Siria. Dimensiunea cibernetică nu oferă acea unealtă universal valabilă care să neutralizeze forțele inamicului, astfel încât să nu mai fie nevoie ca să se desfășoare acțiuni convenționale. În cazul Israelului, dimensiunea cibernetică a fost utilizată în sprijinul și pentru a facilita acțiunile aeriene. După executarea unui atac cibernetic care a facilitat dezactivarea punctuală a apărării aeriene siriene la locul și momentul dorit, a urmat acțiunea convențională de bombardament al obiectivelor vizate. Diferențele dintre cele două momente sunt destul de mari, în primul rând, între cele două state nu exista un război convențional în desfășurare, iar problematica cibernetică nu era atât de intens dezbătută, putem spune chiar că abordarea apărării cibernetice era destul de incipientă.

James Cummins (2022, p. 73) identifica necesitatea considerării domeniului cibernetic ca o problemă de ansamblu a misiunilor forțelor aeriene, nu doar pentru componenta de IT, crescând, astfel, relevanța domeniului pentru comandanții militari NATO. Chiar și pentru cele mai *„simple”* misiuni pe timp de pace, asigurarea serviciului de poliție aeriană, domeniul cibernetic are o importanță deosebită, interacțiunile fiind complexe, începând de la monitorizarea spațiului aerian, procesul de luare a deciziilor în timp foarte scurt, decizia de decolare a aeronavelor pentru controlul situațiilor în care sunt detectate încălcări ale spațiului aerian și până la finalizarea misiunii aeronavelor, prin asigurarea controlului neîntrerupt. Cummins justifică necesitatea tratării domeniului cibernetic ca o problemă de ansamblu a misiunii prin două aspecte, atât prin complexitatea misiunii executate, cât și prin faptul că sunt utilizate componente ale domeniului cibernetic din afara spațiului cibernetic aparținând NATO, incluzând aici rețelele naționale, infrastructura civilă și sistemele informaționale de la bordul aeronavelor și bazelor de pe care acestea operează.

Asigurarea securității cibernetice cu accent pe misiune (Ib.) aduce multe beneficii în ceea ce privește procesul de luare a deciziei de executare a unei misiuni, prin înțelegerea mai bună a mediului de operare, a amenințărilor și riscurilor din punct de vedere cibernetic la adresa misiunii. Înțelegerea modului în care amenințările și vulnerabilitățile cibernetice cresc riscurile de executare a misiunii conduce la o aplicare mult mai eficientă a efectelor cibernetice, iar această interacțiune între misiune și spațiul cibernetic introduce necesitatea operațiilor cibernetice executate

în sprijinul executării misiunii. Înțelegerea situației aeriene ca suport pentru executarea misiunii în mod tradițional a concentrat atenția asupra componentelor rețelelor care există în spațiul fizic și mai puțin asupra domeniului virtual, care este mai greu de conceptualizat. Din punct de vedere al domeniului cibernetic, comandanții trebuie să poată prevedea care dintre modificările din spațiul cibernetic ar putea periclita executarea unei misiuni viitoare, având în vedere atât acțiunile proprii, cât și pe cele ale adversarului.

STUDIU DE CAZ: CONFLICTUL DIN UCRAINA

Utilizarea atacurilor cibernetice a fost unul dintre cele mai noi instrumente identificate a fi folosite de către Rusia, în acest caz fiind foarte ușor pentru Rusia să considere spațiul cibernetic ca fiind o prelungire a granițelor teritoriale (Caimeanu). Din acest punct de vedere, nu observăm mari diferențe în ceea ce privește politica Rusiei în domeniul cibernetic față de modul în care privește Ucraina în domeniul fizic, în ambele cazuri Rusia dorind să treacă peste granițele recunoscute la nivel oficial între cele două state și să ocupe în mod ilegal noi teritorii care nu-i aparțin.

Jakub Przetacznik (2022) a realizat un raport pentru Parlamentul European în care analizează activitățile cibernetice executate de către Rusia asupra Ucrainei. În cadrul raportului este evidențiat faptul că, deși războiul a fost declanșat de către Rusia împotriva Ucrainei la data de 24 februarie 2022, activitățile cibernetice ruse au fost executate în mod continuu de la anexarea ilegală a Peninsulei Crimeea, în anul 2014, și au fost intensificate înainte de declanșarea invaziei din februarie 2022. Acțiunile cibernetice cu efecte vizibile au vizat diferite elemente aparținând infrastructurii ucrainene, dar, cu siguranță, au fost executate și activități cibernetice care au vizat obținerea de acces neautorizat în sistemele informatice ucrainene, precum și sustragerea de date și informații.

Înainte cu o oră de debutul invaziei, a fost executat un atac cibernetic asupra sistemelor de comunicații prin satelit, atac care a condus la întreruperi în asigurarea comunicațiilor pentru persoane fizice, precum și pentru entități publice și private ucrainene. De asemenea, au fost executate atacuri care au vizat rețelele de furnizare a energiei electrice, încercări de distrugere sau perturbare a rețelelor agențiilor guvernamentale, în unele cazuri executând și atacuri cu rachete asupra obiectivelor vizate, scopul urmărit fiind, probabil, subminarea voinței politice a Ucrainei și capacitatea acesteia de a lupta, colectând, în același timp, informații care ar putea oferi avantaje tactice sau strategice forțelor ruse (Lapienyte, 2022). Aproximativ 40% din atacurile care au creat pagube în interiorul infrastructurii ucrainene au vizat organizații din sectoare de infrastructură critică ce ar fi putut avea efecte negative secundare asupra guvernului, armatei, economiei și populației,

la nivel național, regional sau localizat în orașe (Microsoft report, 2022, pp. 2-3). Conform datelor prezentate în raport, Microsoft estimează că activitatea grupurilor ruse de prepoziționare în mediul cibernetic ca parte a pregătirilor pentru conflict a început să se desfășoare cu un an înainte, activitatea cibernetică vizând securizarea accesului pentru colectarea de informații la nivel strategic și operațional, precum și facilitarea executării de atacuri asupra infrastructurii Ucrainei pe timpul conflictului militar (Ib., p. 4).

Atacurile cibernetice executate au vizat atât ținte din Ucraina, cât și din străinătate, inclusiv din state membre ale NATO, activitatea executată pe parcursul anului 2021 constând în activități de spionaj la nivel mai larg. La începutul anului 2022, activitatea cibernetică distructivă s-a intensificat și a cunoscut un vârf al activităților cibernetice înainte de declanșarea invaziei, programe malițioase dezvoltate special pentru sistemele vizate fiind injectate în sistemele ucrainene.

După declanșarea invaziei, activitatea cibernetică rusă identificată a executat misiuni în sprijinul obiectivelor militare strategice și tactice, dar fără a fi foarte clar dacă au existat coordonare, sarcini centralizate sau un set comun de priorități (Grossman, Kaminska, Shires, Smeets, 2023, p. 11). În unele cazuri, atacurile cibernetice au fost executate înainte de un atac militar convențional, dar aceste cazuri identificate au fost rare. Acțiunile din domeniul cibernetic au fost acțiuni de degradare, perturbare sau discreditare a guvernului, armatei ucrainene, agenților economici sau elementelor de infrastructură critică. La data de 6 martie, forțele armate ruse au lansat opt rachete asupra aeroportului Vinnytsa, anterior, la 4 martie, atacul cibernetic a compromis rețelele guvernamentale din domeniul aerian utilizate în Vinnytsa (Microsoft report, p. 7).

Analiza datelor disponibile a reliefat faptul că grupările ruse au acționat în aceleași sectoare sau puncte geografice în care au fost executate în același timp lovituri militare cinetice pentru primele șase săptămâni ale invaziei.

Contrar celor așteptate în primele etape ale războiului dintre Ucraina și Rusia, deși majoritatea experților considerau că acțiunile cibernetice joacă un rol important în cadrul acțiunilor de luptă, nu au fost observate activități intense în domeniul cibernetic. Raportul Microsoft prezintă o mare parte din aceste activități cibernetice, fără a avea pretenția de a fi complet. Majoritatea experților susțin evaluarea că, pentru a înțelege magnitudinea acțiunilor cibernetice, trebuie ca acest război să se încheie și să mai treacă o anumită perioadă de timp pentru dezvăluirea cât mai completă a succesiunii de evenimente. Cu toate acestea, este evident că, fără a fi consultate ambele părți aflate în conflict, va fi dificil de avut această imagine completă, iar la modul cum se desfășoară acest conflict la acest moment, pare destul de improbabil ca atât partea ucraineană, cât și cea rusă să fie dispuse să dezvăluie elemente cu adevărat sensibile privind acțiunile desfășurate.

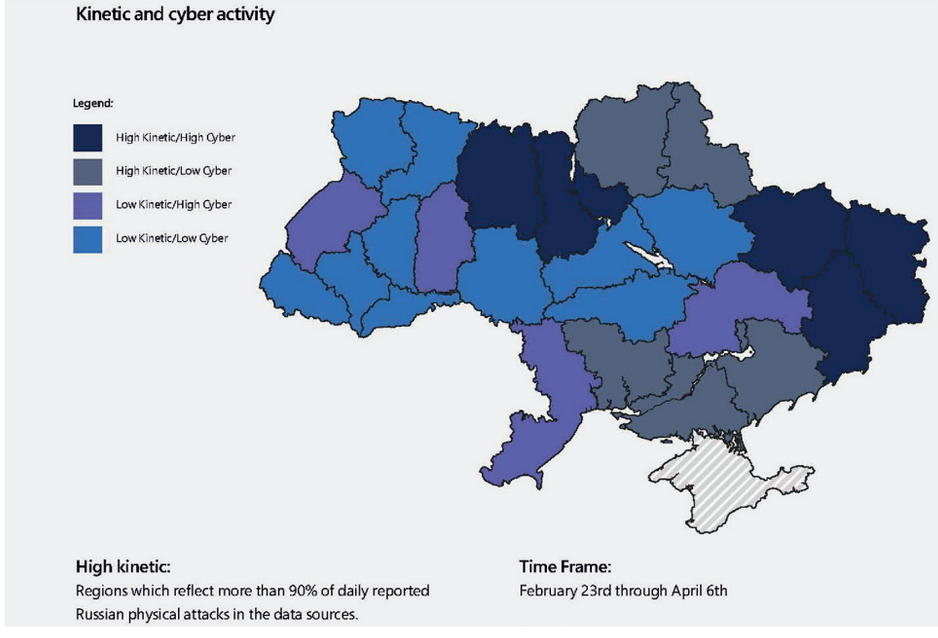

Figura 2: Corelarea activităților cibernetice cu acțiunile militare convenționale (Ib., p. 9).

Dezvoltarea infrastructurii digitale la un nivel accelerat a permis accesul la tehnologie de vârf mult mai ușor comparativ cu accesul la tehnologie de vârf în domeniul aviației. Este de înțeles de ce este protejat accesul la tehnologie de vârf în domeniul aviației, atât din punct de vedere economic, dar mai ales din punct de vedere al asigurării securității statelor și de menținere a avansului tehnologic față de potențialii adversari. Utilizarea pe scară largă a infrastructurii digitale în numeroase domenii, cu toate că și în acest caz există limitări cu privire la accesul la tehnologie de ultimă oră, a permis o mai mare răspândire comparativ cu domeniul de nișă al forțelor aeriene.

Forțele aeriene își desfășoară activitățile pentru a fi în măsură să-și execute misiunile încredințate, dar și pentru a gestiona viitoarele amenințări asociate operării în medii contestate, atât din punct de vedere convențional, cât și cibernetic. Aceasta implică un efort continuu, susținut, la toate nivelurile, atât în ceea ce privește forțele luptătoare, dar mai ales la nivelul comandanților. Schimbarea mentalității este un proces dificil, care nu se întâmplă rapid, dar care este extrem de necesar în contextul evoluției extrem de volatile a mediului de securitate.

Ca urmare a necesității de protejare a forțelor aeriene ucrainene, în condițiile superiorității forțelor aeriene ruse, conducerea ucraineană a luat decizia dispersării

forțelor și mijloacelor atât pe aerodromurile de bază, cât și pe locațiile de rezervă. Ca urmare, a apărut necesitatea asigurării securității cibernetice în mod diferit față de modul în care se asigura la nivel de bază aeriană, centralizat. În opinia mea, transferul de la asigurarea securității cibernetice ca ansamblu la asigurarea misiunii a apărut în mod firesc, ca urmare a diminuării forțelor și resurselor aflate la dispoziție pe locațiile de rezervă. La nivel tactic, misiunile de zbor implică luarea unor decizii extrem de rapid, pe baza unor informații de cele mai multe ori incomplete, care pot să se dovedească mai târziu a fi bune sau total greșite. Din acest punct de vedere, dimensiunea cibernetică este foarte importantă, la nivel tactic comandanții au la dispoziție și alte opțiuni pentru a încerca rezolvarea unei situații care, în mod obișnuit, ar necesita executarea unei acțiuni ofensive convenționale.

Din punct de vedere strategic, dimensiunea cibernetică este foarte dinamică și contestată, evoluțiile domeniului cibernetic din mediul civil fiind utilizate și în mediul militar, iar diferențele din domeniul cibernetic fiind mult mai ușor de acoperit decât în cazul domeniului aerian. Constituirea unor forțe aeriene convenționale necesită mult mai mult timp și resurse decât este cazul domeniului cibernetic. Dimensiunea cibernetică poate fi utilizată concomitent cu alte capabilități militare, fapt care determină atractivitatea crescută a domeniului, atât din perspectiva rezultatelor care pot fi obținute, cât și din perspectiva nivelului mai redus de risc comparativ cu operațiile aeriene ofensive clasice. Pornind de la asigurarea misiunii și, implicit, a aeronavei sau pachetului de aeronave utilizat, forțele aeriene ucrainene au construit securitatea cibernetică în ansamblu, o abordare adaptată resurselor disponibile la nivel strategic, dar adaptată la realitățile de la nivel tactic.

Conflictul din Ucraina a demonstrat, fără echivoc, că viitoarele confruntări vor avea o dimensiune cibernetică. Raportul Microsoft, chiar și incomplet din punct de vedere al datelor colectate sau la care au avut acces experții pe timpul prezenței în Ucraina, a arătat că această dimensiune cibernetică s-a manifestat înainte de începerea conflictului convențional. Activitățile cibernetice nu au fost, de fapt, încetate după preluarea ilegală a Peninsulei Crimeea, în anul 2014, iar intensificarea activității cibernetice semnalate cu multe luni înainte ca atacul convențional să fie declanșat în februarie 2022 nu a constituit o surpriză, atât NATO, cât și Ucraina fiind conștiente de faptul că dimensiunea cibernetică va fi parte integrantă a acestui conflict. Națiunile mai slabe din punct de vedere al capacităților militare convenționale pot utiliza componenta cibernetică drept un multiplicator de forță împotriva națiunilor mai puternice din punct de vedere al capacităților militare, economice și industriale (Stoddart, 2022, p. 29).

INTEGRAREA DOMENIULUI CIBERNETIC ÎN PROCESUL DE PLANIFICARE PE TIMPUL CONFLICTULUI

O forță cibernetică redutabilă poate facilita ca o armată mică să reziste cu succes unei forțe mult mai puternice. Tratarea cu seriozitate a amenințărilor din domeniul cibernetic de către Ucraina, conjugat cu sprijinul extern foarte intens (Cyber Peace Institute, 2023, pp. 15-17), din partea UE, a NATO și a altor actori nonstatali mai mult sau mai puțin dezvoltați, a permis crearea unei apărări cibernetice pe măsura atacatorului. Această defensivă nu a fost creată instantaneu, au fost necesare resurse și eforturi susținute pentru a se reuși acest fapt. Această veritabilă cursă a înarmării a trebuit să țină seamă de integrarea dimensiunii cibernetice în toate etapele desfășurării conflictului, de la planificare, execuție, efecte dorite și cele obținute, atât din perspectiva atacatorului, cât și din perspectiva apărătorului.

Planificarea

Integrarea domeniului cibernetic în planificarea operațiilor aeriene a trebuit să țină cont atât de forțele proprii, cât și de cele ale adversarului, de misiunile dorite, posibile cursuri de acțiune, sprijinul cu informații și, nu în ultimul rând, de dinamica conflictului. Doar simpla enumerare a elementelor care trebuie avute în vedere pe timpul planificării operațiilor aeriene arată amplitudinea problemelor care trebuie rezolvate. Ambele părți aflate în conflict au avut în vedere obiective la nivel strategic foarte diferite. Din perspectiva planificării inițiale, a părut că partea rusă a planificat un conflict care se va încheia rapid și, ca urmare, activitățile cibernetice executate au urmărit în special demonstrarea anumitor capabilități pentru imprimarea unui curs de acțiune din partea ucrainenilor. Posibil, în etapa inițială a conflictului, nu au putut fi evaluate corespunzător capacitățile cibernetice defensive de care dispunea Ucraina, similar cazului forțelor militare convenționale, Rusia nu credea că forțele cibernetice ucrainene sunt pe măsura celor ruse, având în vedere istoricul activităților cibernetice dintre cele două forțe, libertatea de manevră a grupările cibernetice ruse care operau în sistemele ucrainene permițând executarea de activități cibernetice destul de facil.

Execuția

Dacă, în ceea ce privește domeniul aerian, neutralizarea unui obiectiv prin utilizarea mijloacelor convenționale poate fi evaluată ca urmare a vizibilității efectelor produse de utilizarea armelor cinetice, în ceea ce privește domeniul cibernetic, certificarea faptului că un sistem inamic este neutralizat prin utilizarea unor arme cibernetice este mult mai dificilă. Succesul în domeniul cibernetic poate fi permanent, ca în cazul utilizării armamentului convențional, dar la fel de bine

poate fi doar temporar, ca urmare, ar fi benefic dacă ar exista și alte modalități de a confirma succesul unei operații cibernetice.

În acest caz, Ucraina a reușit să integreze foarte eficient ajutorul extern primit de la partenerii internaționali, pe măsura derulării conflictului reușind să blocheze eficient activitățile cibernetice ale adversarului sau, în situația în care nu a fost posibilă aceasta, a reușit totuși să blocheze inițiativele acestuia de confirmare a efectelor atacurilor cibernetice. Ulterior, ca urmare a imposibilității obținerii efectelor dorite de către partea rusă prin intermediul dimensiunii cibernetice, forțele aeriene ruse au trecut la executarea de misiuni de bombardament convențional asupra obiectivelor forțelor aeriene ucrainene.

Efectele dorite

În funcție de efectele dorite, ar trebui să existe o coordonare extrem de precisă atât în ceea ce privește integrarea dimensiunii cibernetice în operațiile aeriene, cât și o coordonare cu celelalte domenii, terestru, maritim, care ar putea să acționeze simultan și să interfereze/interacționeze în ceea ce privește efectele dorite. Din acest punct de vedere, este necesară deconflictarea atât la nivel de specialiști, cât și la nivel de comandanți, pe fiecare palier. Problematica este deosebit de complexă și dificil de rezolvat, iar efectele dorite pot fi la nivel strategic, operațional sau tactic. Cu cât nivelul dorit este mai ridicat, cu atât este mai probabil ca dimensiunea cibernetică din cadrul forțelor aeriene să perturbe sau sa fie perturbată de acțiunile din alte domenii. Din perspectivă ucraineană, coordonarea în ceea ce privește efectele dorite a fost mai ușor de realizat, conducerea forțelor a fost unitară, spre deosebire de partea rusă, unde au fost implicate diferite entități cibernetice, statale și nonstatale. Cel puțin în etapele de început ale conflictului, entitățile ruse au acționat destul de haotic, fără a fi realizată o coordonare eficientă privind efectele dorite și modul în care acestea pot fi obținute.

Efecte obținute

Conflictul din Ucraina a demonstrat cât de greu este de executat o operație întrunită pe mai multe direcții de acțiune. Pe acest fond, includerea dimensiunii cibernetice ridică noi provocări în ceea ce privește efectele obținute din punct de vedere al utilizării dimensiunii cibernetice în mod întrunit. Dimensiunea cibernetică trebuie să asigure atât securitatea națională din punct de vedere cibernetic, cât și să execute acțiuni cibernetice ofensive asupra facilităților și infrastructurii adversarului. Din acest punct de vedere, efectele dorite de către partea rusă la începutul conflictului nu au fost obținute. Chiar și din puținele informații disponibile, se poate observa că a avut loc o tranziție de la executarea de atacuri cibernetice ruse asupra facilităților ucrainene la o ripostă ucraineană asupra facilităților ruse.

Aceasta poate semnaliza maturizarea apărării cibernetice ucrainene, care acum se simte în măsură să apare din punct de vedere cibernetic infrastructura proprie și a trecut la executarea de acțiuni ofensive atât pentru a sprijini acțiunile ofensive ale forțelor armate ucrainene, cât și pentru a deturna forțe și mijloace ruse de la executarea de acțiuni ofensive la acțiuni defensive pentru apărarea facilităților și infrastructurii de pe teritoriul național rus.

În ceea ce privește efectele obținute, a fost observată atât tendința de a reacționa simetric la acțiunile adversarului, cât și reacția de a utiliza mijloacele evaluate ca fiind cele mai potrivite pentru a răspunde deopotrivă prin atacuri convenționale și atacuri cibernetice, indiferent de metoda de atac aleasă de adversar.

Ucraina a dat dovadă de multă ingeniozitate în folosirea mijloacelor aflate la dispoziție pentru apărarea teritoriului național. Contribuția dimensiunii cibernetice la continuarea executării misiunilor de către forțele aeriene ucrainene nu poate fi evaluată la adevărata ei valoare, dar se poate afirma că domeniul cibernetic este unul dintre pilonii care susțin securitatea forțelor aeriene ucrainene și, implicit, asigurarea securității naționale pentru Ucraina. Chiar dacă, la nivel global, Ucraina era situată mult sub poziția Rusiei în ceea ce privește domeniul cibernetic, a reușit ca, în timpul foarte scurt avut la dispoziție și sub presiunea continuării războiului, cu sprijin substanțial extern, să-și construiască o apărare cibernetică pe măsura amenințării ruse.

CONCLUZII

Forțele aeriene sunt, prin natura lor, o forță foarte tehnologizată și care a beneficiat de implementarea ultimelor inovații din domenii diverse, foarte rapid de la apariția acestora pe piață. Ca urmare, forțele aeriene, ca lider în domeniul inovării, au recunoscut destul de devreme importanța domeniului cibernetic pentru activitățile desfășurate, atât din punct de vedere defensiv, cât și din punct de vedere ofensiv. Domeniul cibernetic a adus o mulțime de avantaje forțelor aeriene, dar, în același timp, a venit la pachet cu noi vulnerabilități și riscuri asociate. Abordarea militară a securității cibernetice, care pleacă de la nivel strategic la nivel tactic în ceea ce privește asigurarea protecției infrastructurii critice, este ușor diferită de abordarea din mediul privat, care privește asigurarea protecției infrastructurii critice din perspectivă mai ales economică. Influența domeniului cibernetic asupra forțelor aeriene nu poate fi privită ca abordare pur militară sau pur civilă, ca urmare, în activitățile forțelor aeriene trebuie luat în considerare faptul că acțiunile cibernetice malițioase sunt rezultatul acțiunii unor state ostile. Asigurarea securității infrastructurii critice pentru forțele aeriene are o legătură directă cu asigurarea securității naționale, prin asigurarea operării forțelor aeriene în asigurarea protecției

spațiului aerian național. În opinia mea, domeniul cibernetic este important și de actualitate pentru activitatea forțelor aeriene, studiul de caz demonstrând acest fapt, fiind necesară, în același timp, o recalibrare a modului în care este privit domeniul cibernetic din punctul de vedere al asigurării misiunii ca element central al securității cibernetice.

Resursele limitate, precum și alocarea acestora spre rezolvarea tuturor problemelor considerate urgente au condus la o constrângere a domeniului cibernetic, simpla existență a unor structuri destinate apărării cibernetice fiind considerată a fi suficientă.

Cu toate acestea, conflictul din Ucraina a arătat că, deși la nivel teoretic importanța domeniului cibernetic a fost recunoscută și au existat inițiative în domeniu pentru asigurarea securității cibernetice, aceasta nu a fost suficient. Așa cum a fost evidențiat în raportul Microsoft, actorii cibernetici ostili au exploatat mult mai eficient domeniul cibernetic, activitatea malițioasă din domeniul cibernetic practic a fost mai mereu la niveluri ridicate, aspect evidențiat de impactul atacurilor cibernetice executate. În cazul unui actor cibernetic statal de calibrul Rusiei, a fost nevoie de un efort susținut din partea Ucrainei, care a fost impulsionată de necesitățile stringente ale războiului pentru a atinge un nivel satisfăcător al securității cibernetice. Este evident, astfel, că dimensiunea cibernetică va fi o componentă a viitoarelor conflicte, în opinia mea, în condițiile avansului tehnologic din ce în ce mai rapid, pentru a asigura supraviețuirea elementelor forțelor aeriene, iar locul și rolul dimensiunii cibernetice în cadrul activităților forțelor aeriene vor crește.

Imposibilitatea asigurării supremației aeriene pentru forțele aeriene ruse, chiar și în condițiile unei activități în domeniul cibernetic destul de intense, pe perioade extinse de timp, demonstrează importanța asigurării unei defensive eficiente, dar, în același timp, așteptările privind capacitățile defensive și pe cele ofensive nu trebuie să fie supraestimate. Având în vedere resursele disponibile, chiar dacă la nivel național integrarea dimensiunii cibernetice trebuie privită din perspectivă strategică, pe baza studiului de caz, ar trebui aprofundate metodele prin care să se asigure securitatea cibernetică centrată pe asigurarea misiunii.

Posibil, centrarea pe asigurarea misiunii, din punct de vedere, cibernetic a forțelor aeriene ucrainene, în condițiile în care au fost acceptate ca fiind rezonabile niveluri ridicate de risc, a permis continuarea executării misiunilor de zbor pe tot parcursul conflictului dintre cele două state. Așa cum a demonstrat și continuă să demonstreze războiul dintre Ucraina și Rusia, influența dimensiunii cibernetice asupra activității forțelor aeriene ucrainene nu poate fi neglijată, acest fapt contribuind implicit și la asigurarea securității naționale pentru Ucraina.

BIBLIOGRAFIE:

1. *An overview of Russia's cyberattack activity in Ukraine. Special Report Ukraine, Microsoft* (2022), pp. 2-3, https://aka.ms/ukrainespecialreport, accesat la 10 iunie 2023.
2. Caimeanu, M. (2021). *A cincea dimensiune. Rolul spațiului cibernetic în gândirea strategică a Federației Ruse*, http://ispri.ro/a-cincea-dimensiune-rolul-spatiului-cibernetic-in-gandirea-strategica-a-federatiei-ruse/, accesat la 9 iunie 2023.
3. Cummins, J. (2022). *Addressing Cyber Challenges Through the Prism of The NATO Air Policing Mission*, https://www.jwc.nato.int/newsroom/The-Three-Swords-Magazine/three-swords-38, accesat la 28 septembrie 2023.
4. Cyber Peace Institute (2023). *Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q1 January to March 2023*, https://cyberpeaceinstitute.org/wp-content/uploads/2023/05/Ukraine-Report-Q1_FINAL.pdf, accesat la 11 iunie 2023.
5. Grossman, T., Kaminska, M., Shires, J., Smeets, M. (2023). *The Cyber Dimensions of the Russia-Ukraine War,* https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf., accesat la 10 iunie 2023.
6. Lapienyte, J. (2022). *Russia correlates cyberattacks with its kinetic military operations in Ukraine – Microsoft, 2022,* https://cybernews.com/cyber-war/russia-correlates-cyberattacks-with-its-kinetic-military-operations-in-ukraine-microsoft/, accesat la 9 iunie 2023.
7. Lilly, B. (2022). *Russian Information Warfare: Assault on Democracies in the Cyber Wild West*, Naval Institute Press,
8. Microsoft (2022). *An overview of Russia's cyberattack activity in Ukraine, Special Report Ukraine, Microsoft*, https://aka.ms/ukrainespecialreport, accesat la 9 iunie 2023.
9. Przetacznik, J. (2022). *Războiul Rusiei împotriva Ucrainei: Cronologia atacurilor cibernetice*, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(202)733549, accesat la 6 iunie 2023.
10. Raffray, E., Millochau, G. (2023). *War in Ukraine computer network control and impact on civilians*, https://cyberpeaceinstitute.org/publications/war-in-ukraine-computer-network-control-and-impact-on-civilians/, accesat la 11 iunie 2023.
11. Stoddart, K. (2022). *Cyberwarfare, Threats to Critical Infrastructure*. Editura Palgrave Macmillan.
12. Timea, P., Skopik, F. (2018). *Collaborative Cyber Threat Intelligence.* Editura CRC Press.
13. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM23-Mar-18.pdf, p. 3, accesat la 18 septembrie 2023.