Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 11 (190) / 2021
Indexat în
CEEOL și ROAD

TEHNOLOGII ÎN CURS DE DEZVOLTARE CARE POT INFLUENȚA SECURITATEA CIBERNETICĂ ÎN INFRASTRUCTURILE MILITARE DE COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI. STUDIU DE CAZ – TEHNOLOGIA DE REȚEA 5G

Ovidiu-Dumitru RUSU

Developing technologies that can influence cyber security in military communications infrastructures and information technology. Case study – 5G network technology

Abstract: *Developing technologies, also known as emerging technologies, can influence the security of cyberspace. New emerging technologies that can influence cybersecurity are artificial intelligence, the development of human-robot interfaces, lethal autonomous systems and devices, quantum computers and communications, data storage technologies, sensors and communications technologies through 5G network technology, satellite systems, machine learning equipment, etc.*

More and more state actors are involved in the research and development of these new emerging technologies. The implementation of developing technologies in civil and military communications and information technology infrastructures is a priority for state actors, but the advantages and disadvantages they offer to cyberspace must be taken into account. In the scientific research we are carrying out, using in particular the observation method applied to developing technologies, we will analyze the current level of concern for ensuring cyber security in military operational communications infrastructures and information technology through network technology. 5G.

We submit this research issue for analysis on the grounds that some of the developing technologies will significantly influence the cyber security of military operational communications infrastructures and information technology through 5G network technology.

Keywords: *emerging technologies, cyberspace, 5G network technology, communications infrastructure and information technology, cybersecurity.*

Tehnologii în curs de dezvoltare care pot influența securitatea cibernetică în infrastructurile militare de comunicații și tehnologia informației. Studiu de caz – tehnologia de rețea 5G

Rezumat: *Tehnologiile aflate în curs de dezvoltare (inteligența artificială, dezvoltarea interfețelor om-roboți, sistemele și dispozitivele autonome letale, calculatoarele și comunicațiile cuantice, tehnologiile de stocare a datelor, senzorii și tehnologiile de comunicații prin tehnologia de rețea 5G, sistemele satelitare, echipamentele cu învățare automată etc.), cunoscute și sub denumirea de tehnologii emergente, pot influența securitatea spațiului cibernetic.*

Tot mai mulți actori statali sunt implicați în cercetarea și dezvoltarea acestor noi tehnologii. Implementarea tehnologiilor în curs de dezvoltare în infrastructurile civile și militare de comunicații și tehnologia informației reprezintă o prioritate pentru actorii statali, însă trebuie avute în vedere avantajele și dezavantajele pe care acestea le oferă spațiului cibernetic. În demersul de cercetare științifică pe care îl realizăm, prin folosirea în special a metodei observației aplicată tehnologiilor în curs de dezvoltare, vom analiza gradul de preocupare existent la acest moment pentru asigurarea securității cibernetice în infrastructurile militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G.

Supunem această problemă de cercetare spre analiză din motivația că o parte a tehnologiilor în curs de dezvoltare vor influența în mod semnificativ asigurarea securității cibernetice a infrastructurilor militare operative de comunicații și tehnologia informațiilor prin tehnologie de rețea 5G.

Cuvinte-cheie: *tehnologii emergente, spațiu cibernetic, tehnologie de rețea 5G, infrastructuri de comunicații și tehnologia informației, securitate cibernetică.*

***Ovidiu-Dumitru RUSU** este doctorand în domeniul „Informații și securitate națională” în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: rusuodumitru@yahoo.com).*

Introducere

Amenințările și vulnerabilitățile manifestate în infrastructurile militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G dobândesc noi forme și valențe ceea ce complică și mai mult asigurarea unui spațiu cibernetic funcțional, normal și sigur.

Realitățile cotidiene ne dovedesc faptul că activitățile umane sunt tot mai dependente de funcționarea la parametri optimi a spațiului cibernetic. De exemplu, multe dintre sectoarele de activitate migrează, cu pași mici, dar siguri, parțial sau total, către lucrul în mediul online. De aceea, menținerea unui spațiu cibernetic în stare de funcționalitate reprezintă un deziderat pe care fiecare actor statal sau non-statal de bună credință ar trebui să și-l dorească.

Astăzi, mai mult decât oricând, avem nevoie de soluții viabile care să ne permită să desfășurăm activitățile dependente de infrastructurile de comunicații și tehnologia informației în condiții de normalitate cibernetică.

Structurile militare, la fel ca celelalte domenii de activitate (energie, transport, financiar, sănătate, educație etc.) și-au transferat o parte din activitățile curente în mediul online. Dezvoltarea învățământului online, desfășurarea unor manifestări științifice în sistem de videoconferință sau realizarea altor activități specifice cu ajutorul sistemelor informatice ne dovedesc faptul că modul de comunicare prin intermediul tehnologiilor actuale este tot mai uzual, oferind în același timp o multitudine de avantaje.

Pentru asigurarea securității spațiului cibernetic avem nevoie de dezvoltarea și implementarea tehnologiilor emergente în arhitecturile integrate de securitate cibernetică. Susținute de noile tehnologii (inteligența artificială, comunicații și calculatoare cuantice, sisteme cu învățare automată etc.), aceste noi arhitecturi pot fi mult mai eficiente în combaterea atacurilor cibernetice.

1. Tehnologiile în curs de dezvoltare care pot influența securitatea cibernetică

În decursul evoluției civilizației umane, ființa umană prin capacitățile intelectuale pe care le posedă a creat în permanență noi tehnologii care au asigurat progresul societății. Fără o dezvoltare continuă a tehnologiilor nu am fi putut înregistra salturi calitative în sectoarele de activitate. Diversitatea tehnologiilor și îmbunătățirea continuă a acestora ne-a permis să obținem progrese remarcabile în toate domeniile de activitate.

Cu toate că progresul tehnologic în anumite sectoare de activitate a înregistrat și efecte negative la nivel mondial (poluare, schimbări climatice, extincția anumitor specii de plante și animale), necesitatea unor salturi tehnologice a avut câștig de cauză.

Urmare a demersurilor de cercetare științifică efectuate de către Jacobs Bellasio și Erik Silversten, autorii articolului *The impact of new and emerging and technology on the cyber threat landscape and their implications for NATO (Impactul tehnologiilor noi și emergente asupra tabloului amenințărilor cibernetice și implicațiile acestora pentru NATO)*, s-a ajuns la concluzia că principalele tehnologii în curs de dezvoltare care pot afecta securitatea spațiului cibernetic al statelor membre ale Alianței Nord-Atlantice sunt următoarele:

a) inteligența artificială și dezvoltarea interfețelor om-roboți;

b) sistemele și dispozitivele autonome;

c) tehnologiile de stocare a datelor, senzorii și tehnologiile de telecomunicații;

d) comunicațiile prin sateliți;

e) echipamentele cu învățare automată;

f) calculatoarele și comunicațiile cuantice.[1]

În noiembrie 2020, Serviciul pentru cercetare al Congresului american a publicat Raportul *Emerging Military Technologies: Background and Issues for Congress (Tehnologii militare emergente: Context și probleme pentru Congres)* în care au fost prezentate principalele tehnologii militare emergente care se află în atenția SUA, Chinei și Federației Ruse. Potrivit Raportului, cele trei state și-au focusat atenția pe dezvoltarea următoarelor tehnologii emergente: „inteligența artificială, arme autonome letale, arme hipersonice, arme cu energie dirijată, biotehnologie și tehnologie cuantică”[2].

Comparând rezultatele cercetărilor obținute de autorii celor două publicații *The impact of new and emerging and technology on the cyber threat landscape and their implications for NATO, respectiv Emerging Military Technologies: Background and Issues for Congress,* observăm că dezvoltarea tehnologiilor de inteligență artificială și cele cuantice reprezintă un interes major pentru forțele armate ale SUA și, implicit, NATO.

Tehnologiile de inteligență artificială se bucură de o atenție deosebită în ultima perioadă, tocmai datorită faptului că s-a constatat că acestea oferă nenumărate posibilități și oportunități ce pot sprijini dezvoltarea capabilităților militare, cu performanțe vizibil mai bune comparativ cu cele ale ființei umane. Simbioza dintre inteligența artificială și

[1] BELLASIO, Jacobs, and SILVERSTEN, Erik, *The impact of new and emerging and technology on the cyber threat landscape and their implications for NATO, Cyber threats and NATO 2030: Scanning and analysis*, NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE, 2020, pp. 90-95.

[2] ***, Congressional Research Service, *Emerging Military Technologies: Background and Issues for Congress*, URL: https://fas.org/sgp/crs/natsec/R46458.pdf, 10 november 2020, accesat la 19.07.2021, p. 2.

celelalte tehnologii emergente va conduce, cel mai probabil, la o redimensionare a spațiului de luptă din punctul de vedere al forțelor militare participante la executarea operațiilor inteligente. În următoarele decenii, inteligența artificială, alături de comunicațiile cuantice, vor reprezenta vârful de lance în dezvoltarea celorlalte tehnologiilor emergente.

Deși în mediul militar se vorbește mai puțin decât în mediul civil despre implementarea tehnologiei 5G, este posibil ca în viitorul apropiat să asistăm la o creștere exponențială a dispozitivelor militare conectate la infrastructurile de comunicații și tehnologia informației, ceea ce ar presupune folosirea unor benzi mai largi de frecvențe.

Conectarea tuturor echipamentelor / platformelor de luptă care acționează în câmpul tactic la infrastructurile militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G prezintă o serie de probleme care țin de asigurarea securității spațiului cibernetic. Una dintre întrebările pertinente care privesc problemele majore de securitate cibernetică ar putea fi: *Ce se va întâmpla dacă adversarul prin mijloacele pe care le are la dispoziție ar putea prelua controlul unor echipamente/platforme de luptă proprii conectate la infrastructura militară operativă de comunicații și tehnologia informației prin tehnologia de rețea 5G?*

Cel mai probabil, o infrastructură militară operativă de comunicații și tehnologia informației realizată prin tehnologie de rețea 5G prezintă și o serie de vulnerabilități specifice acțiunilor de atac cibernetic și operațiilor de război electronic. Cele mai importante vulnerabilități sunt generate de faptul că transmisiile se realizează prin unde radio, permit conectarea unui număr foarte mare de dispozitive la rețea și se bazează pe mai multe puncte de rutare ale traficului pachetelor de date și pe „*exploatarea punctelor slabe ale protocoalelor de interconectare*”[3]. Fără îndoială, adversarul va încerca să utilizeze alături de alte operații specifice și întreaga gamă de operații cibernetice și de război cibernetic pentru a obține supremația informațională în spațiul cibernetic.

În acest sens, apreciem că planificarea, organizarea și executarea operațiilor de război cibernetic și război electronic ar trebui să se realizeze astfel încât misiunile să nu se suprapună, iar în acest mod să se obțină o economie a forțelor și mijloacelor angrenate în conflict.

2. Tehnologia de rețea 5G la nivelul Uniunii Europene. Avantaje și dezavantaje

În ianuarie 2020, Comisia Europeană a adoptat documentul intitulat *Implementarea rețelelor 5G în condiții de siguranță în Uniunea Europeană – Punerea în aplicare a setului de instrumente al Uniunii Europene*[4].

În capitolul doi al acestui document, *Introducerea tehnologiei 5G în UE*, se precizează că „*implementarea infrastructurii de rețea 5G în Europa este esențială pentru strategia și competitivitatea industrială europeană. [...] implementarea tehnologiilor de rețea 5G reprezintă un factor major pentru facilitarea serviciilor digitale viitoare*”[5]. Din cele menționate, rezultă faptul că dezvoltarea tehnologiilor de rețea 5G reprezintă o prioritate pentru UE în scopul dezvoltării infrastructurilor de comunicații și tehnologia informației existente. Totodată, oficialii de la Bruxelles au elaborat și un set de instrumente pentru asigurarea securității cibernetice a infrastructurilor de comunicații și tehnologia informației.

În același document, la capitolul patru, *Setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G*, Comisia Europeană a identificat ca principale măsuri și acțiuni pentru asigurarea securității cibernetice în rețelele 5G, următoarele:[6]

a) măsuri strategice pentru creșterea competențelor de reglementare ale autorităților care să permită monitorizarea achizițiilor publice din domeniul rețelelor, pentru abordarea riscurilor care au legătură cu vulnerabilitățile, dar care nu sunt de natură tehnică, pentru promovarea unui lanț de aprovizionare și valoric 5G sustenabil și diversificat care să evite riscul de dependență sistemică pe termen lung;

b) măsuri tehnice care presupun consolidarea securității rețelelor și echipamentelor 5G printr-o abordare a riscurilor care decurg din tehnologii, procese și factorul uman;

c) elaborarea planurilor de atenuare a riscurilor bazate pe măsuri cu eficacitate maximă.

Tehnologia de rețea 5G a apărut ca o necesitate a dezvoltării infrastructurilor de comunicații și tehnologia informației. În comparație cu tehnologia de rețea 4G, noua tehnologie vine la pachet cu o serie de avantaje care asigură, în primul rând, decongestionarea traficului de date în rețea. Principalele avantaje oferite de tehnologia de rețea 5G în infrastructurile de comunicații și tehno-

[3] ***, *Threat assessment for the fifth generation of mobile telecommunications networks (5G)*, NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE, November 2019, URL: https://www.enisa.europa.eu /publications/enisa-threat-landscape-for-5g-networks, accesat la 20.07.2021, p. 62.

[4] ***, *Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Implementarea rețelelor 5G în condiții de siguranță în Uniunea Europeană – Punerea în aplicare a setului de instrumente al Uniunii Europene*, Comisia Europeană, Bruxelles, 29 ianuarie 2020.

[5] *Ibidem*, p. 1.

[6] *Ibidem*, p. 5.

logia informației ar fi următoarele:

a) viteză de transfer a pachetelor de date mult mai mare;

b) permite conectarea simultană a mai multor dispozitive la infrastructura militară operativă de comunicații și tehnologia informației;

c) reduce semnificativ întârzierile de transfer a pachetelor de date;

d) contribuie la dezvoltarea caselor și a orașelor inteligente;

e) asigură o dezvoltare a producției pentru anumite domenii de activitate.

Ca orice tehnologie nouă implementată, tehnologia de rețea 5G prezintă și o serie de dezavantaje care nu pot fi trecute cu vederea, și anume:

a) distanța de propagare a undelor electromagnetice este mai mică;

b) necesită instalarea mai multor antene într-o anumită arie geografică, tocmai pentru a avea o acoperire mai bună;

c) costurile necesare implementării unei astfel de tehnologii sunt destul de ridicate;

d) realizarea comunicațiilor prin frecvențe de ordinul zecilor și sutelor de GHz poate fi perturbată de anumiți factori naturali sau industriali;

e) conectarea unui număr foarte mare de dispozitive la infrastructura de comunicații și tehnologia informației determină creșterea vulnerabilităților în spațiul cibernetic;

f) creșterea dependenței utilizatorilor de rețea 5G va crea mari probleme în cazul nefuncționării infrastructurilor de comunicații şi tehnologia informației.

Apreciem că interesul crescut al autorităților europene și internaționale pentru implementarea tehnologiilor de rețea 5G are o strânsă legătură și cu dezvoltarea celorlalte tehnologii emergente – inteligența artificială, dispozitivele autonome, comunicațiile și calculatoarele cuantice, echipamente cu învățare automată etc. –, ce necesită transferul unui flux mult mai mare de date și informații.

3. Tehnologia de rețea 5G în mediul militar

La data de 8 octombrie 2020, subsecretarul de stat american al apărării, responsabil pentru domeniile de cercetare și inginerie, Michael Kratsios, a declarat că militari din cadrul forțelor armate americane, împreună cu reprezentanți ai mai multor companii private, testează și experimentează tehnologii de rețea 5G în mai multe locații de pe teritoriul Statelor Unite ale Americii.

Potrivit celor declarate de oficialul american, activitățile vizează următoarele domenii de cercetare:[7]

a) Realitate augmentată/ virtuală – Joint Base Lewis, McChord, Washington;

b) Depozitare inteligentă echipamente specifice forțelor navale – Naval Base San Diego, California;

c) Depozitare inteligentă și întreținere vehicule – Marine Corps Logistics Base Albany, Georgia;

d) Comandă și control distribuite – Nellis Air Force Base Nevada;

e) Utilizare dinamică a spectrului – Hill Air Force Base, Utah.

De asemenea, autorii articolului intitulat *Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation (Asigurarea 5G: rolul NATO în colaborarea pentru evaluarea și diminuarea riscurilor)*, publicat în anul 2020, recomandă Alianței Nord-Atlantice realizarea unei cooperări internaționale în vederea asigurării securității infrastructurilor de comunicații și tehnologia informației care utilizează tehnologie 5G prin:[8]

a) parteneriat internațional pentru evaluarea riscurilor și testarea produselor;

b) partajarea informațiilor despre amenințarea cibernetică;

c) extinderea standardizării către ecosistemul 5G.

Se observă că interesul pentru utilizarea tehnologiei de rețea 5G a crescut, în ultimii ani, și în mediul militar. Specialiștii armatei în colaborare cu cei civili cercetează și experimentează posibilitatea implementării tehnologiilor de rețea 5G în diverse domenii de activitate cu specific militar.

Conectarea tuturor forțelor la o infrastructură militară operativă proprie de comunicații și tehnologia informației bazată pe tehnologie de rețea 5G reprezintă un deziderat care ar permite comandanților să obțină o imagine cât mai completă și, totodată, detaliată a câmpului de luptă modern. De asemenea, tehnologia de rețea 5G ar permite un transfer mult mai rapid al datelor către factorii decidenți, evitând astfel blocajele sau întârzierile specifice a pachetelor de date.

Din punct de vedere tehnic acest lucru este posibil de realizat, însă principala problemă care trebuie soluționată cu tehnologiile prezente se referă la faptul cum va fi asigurată securitatea cibernetică a infrastructurilor militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G care găzduiesc echipamente-

---

[7] ***, *DOD Announces $600 Million for 5G Experimentation and Testing at Five Installations,* US Department of Defense, 8 October 2020, URL: https://www.defense.gov/Newsroom/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati, accesat la 08.06.2021.

[8] DASILVA, Luiz A., H. REED, Jeffrey, SHETTY, Sachin, PARK, Jerry, WIJESEKERA, Duminda, WANG, Haining, *Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation*, NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE, 2020, URL: https://ccdcoe.org/uploads/2020/12/4-Securing-5G_ebook.pdf, accesat la data de 19.07.2021, pp. 82-84.

le/platformele militare. Acesta reprezintă un punct sensibil, o posibilă vulnerabilitate, pentru mediul militar, deși specialiștii în domeniu încearcă să identifice și să implementeze cele mai bune soluții de arhitecturi integrate de securitate cibernetică dedicate asigurării unui spațiu cibernetic funcțional, normal și sigur.

Realizând o simplă estimare, în aria de operații a unei structuri militare de nivel corp de armată am avea câteva zeci de mii de dispozitive care ar putea fi conectate la o infrastructură militară operativă de comunicații și tehnologia informației prin tehnologie de rețea 5G, în condițiile în care am include și resursa umană echipată cu senzori și dispozitive de transmitere a datelor în timp real. Pe de altă parte, fiind vorba de comunicații sau non-comunicații în spectrul electromagnetic trebuie luate în calcul, în mod obligatoriu, și operațiile cibernetice și de război electronic executate de adversar.

Asigurarea compatibilității electromagnetice în scopul evitării producerii interferențelor electromagnetice este o altă problemă identificată, la care structurile de comunicații și tehnologia informației vor trebui să găsească soluții de rezolvare.

Utilizarea dispozitivelor militare autonome, dezvoltarea tehnologiilor de inteligență artificială, implementarea conceptului militar-robot sunt doar câteva dintre inovațiile care completează harta câmpului de luptă modern și care ne îndreptățesc să afirmăm că războaiele viitorului nu se vor mai desfășura în forma lor actuală. Creșterea numărului echipamentelor/platformelor de luptă în aria de operații nu înseamnă că vom avea nevoie de un număr mai mic de militari, ci dimpotrivă, numărul participanților s-ar putea să fie mai mare, iar nivelul de instruire mult mai ridicat. În spatele echipamentelor/platformelor de luptă cu autonomie sporită vor trebui să se regăsească militari bine instruiți și pregătiți, capabili să adopte cele mai bune decizii în condițiile de incertitudine pe care le oferă războiul. Militarul modern va avea mai mult un rol de manager al echipamentelor/platformelor de luptă pe care le gestionează în timpul misiunilor încredințate, folosindu-se în acest scop și de noile tehnologii.

4. Războaie inteligente în contextul evoluției tehnologiei de rețea 5G

Războaiele inteligente aparțin viitorului și se vor desfășura în alte condiții decât cele actuale, tocmai datorită posibilităților și oportunităților pe care le oferă actualele tehnologii emergente în procesul de dezvoltare de noi capabilități militare. Evoluția noilor tehnologii și instalarea acestora pe echipamente/platforme moderne de luptă vor contribui semnificativ la o regândire a modului de distribuție și utilizare a forțelor armate în câmpul de luptă.

Puterile militare încearcă să dețină supremația asupra tehnologiilor în curs de dezvoltare, de aceea în momentul de față, la nivel mondial, state precum SUA, China, Federația Rusă, Coreea de Sud, Israel etc. investesc sume uriașe în programe de cercetare. Un exemplu în acest sens este oferit de investițiile masive efectuate de Departamentul american al apărării în tehnologia de inteligență artificială, care erau estimate „*la circa 600 de milioane de dolari în anul 2016, iar în anul 2020 ... la 927 de milioane de dolari*”[9].

Chiar dacă tehnologia de rețea 5G are și anumite dezavantaje, prezentate în capitolul al doilea al acestei lucrări, avantajele oferite obligă părțile beligerante să le utilizeze în planificarea, organizarea și executarea operațiilor militare inteligente. Implementarea tehnologiei 5G în infrastructurile militare operative de comunicații și tehnologia informației ale forțelor armate va permite conectarea la rețeaua de misiune a unui număr mult mai mare de echipamente/platforme militare care acționează în câmpul tactic, ceea ce va oferi o imagine aproape completă a zonei de operații și va ajuta comandanții să ia cele mai bune decizii într-un timp cât mai scurt. De asemenea, tehnologiile de rețea 5G vor permite recepționarea și transmiterea pachetelor de date într-un volum mult mai mare, la o viteză superioară.

Aproape toate, dacă nu chiar toate tehnologiile militare emergente își vor putea pune în valoare capabilitățile numai dacă și infrastructura militară operativă de comunicații și tehnologia informației prin tehnologie de rețea 5G la care sunt conectate va fi funcțională, normală și ultra securizată.

Un exemplu în acest sens ar putea fi oferit de utilizarea armelor autonome letale într-o situație de criză. În cadrul acestui scenariu, o dronă primește misiunea de a lansa o rachetă asupra unui autovehicul care transportă un lider terorist, cu mențiunea că dronei nu i-au fost acordate privilegii de lansare a rachetei decât cu acordul operatorului uman. După identificarea zonei în care autovehiculul se deplasează, drona pierde legătura cu stația de bază, iar operatorul nu reușește să transmită comanda de lansare a rachetei deoarece frecvențele au fost bruiate. Mai mult decât atât, teroriștii reușesc să preia comanda și controlul acesteia și o transportă către o locație controlată de ei.

Estimăm că, în acest scenariu, principalele cauze care au determinat un asemenea eșec au fost următoarele:

a) frecvențele pe care au fost realizate comunicațiile nu au fost protejate împotriva atacurilor

[9] Congressional Research Service, *Emerging Military Technologies: Background and Issues for Congress*, URL: https://fas.org/sgp/crs/natsec/R46458.pdf, 10 november 2020, accesat la data de 19.07.2021, p. 3

electronice;

b) securizarea insuficientă a transmisiilor comunicațiilor a permis preluarea comenzii și controlul dronei;

c) alegerea unor frecvențe neadecvate zonei în care a acționat drona.

Rezumând cele prezentate în cadrul scenariului observăm că misiunea de luptă nu a putut fi îndeplinită datorită nefuncționării la parametri normali a infrastructurii militare operative de comunicații și tehnologia informației.

Scenariul prezentat este unul simplist, dar realist, având în vedere că într-un conflict armat, fiecare dintre părțile beligerante va încerca să-și adapteze propriile tehnologii la realitățile câmpului de luptă. De aceea, noile echipamente/platforme de luptă și succesul operațiile moderne vor continua să fie tot mai dependente de infrastructurilor militare operative de comunicații și tehnologia informației care vor funcționa și pe baza tehnologiei de rețea 5G.

Problemele actuale ale tehnologiei de rețea 5G vor fi, cel mai probabil, rezolvate în mare parte odată cu dezvoltarea tehnologiilor cuantice și de inteligență artificială. Tehnologiile cuantice vor garanta o criptare/decriptare mult mai sigură a pachetelor de date, în timp ce inteligența artificială va asigura o securitate cibernetică superioară a infrastructurii militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G.

Concluzii și propuneri

Evoluția noilor tehnologii emergente vor influența și modela modul de desfășurare a operațiilor militare în câmpul de luptă, indiferent de nivelul la care se desfășoară: tactic, operativ sau strategic.

Necesitatea de a conecta toate echipamentele/platformele militare aflate în zona de operații, inclusiv senzorii și dispozitivele aflate asupra militarilor, la o infrastructură militară operativă de comunicații și tehnologia informației prin tehnologie de rețea 5G reprezintă o mare provocare din punctul de vedere al asigurării securității cibernetice. Tehnologiile de rețea 5G facilitează această interconectare și reprezintă un avantaj tehnologic major atât pentru societatea civilă, cât și pentru mediul militar.

Identificarea celor mai bune soluții de securitate cibernetică menite să asigure un spațiu cibernetic funcțional, normal și sigur se află în responsabilitatea forțelor specializate de comunicații, tehnologia informației și apărare cibernetică. Conectarea tuturor dispozitivelor militare la o infrastructură militară operativă de comunicații și tehnologia informației prin tehnologie de rețea 5G ar trebui realizată în condiții de maximă securitate cibernetică, astfel încât adversarul să nu aibă posibilitatea să limiteze acțiunile echipamentelor/platformelor militare proprii în câmpul de luptă.

Dacă în societatea civilă utilizăm conceptele de casă inteligentă și oraș inteligent, în același sens, putem utiliza și conceptul de câmp tactic inteligent în operațiile militare, din perspectiva utilizării tehnologiilor de rețea 5G. Deși, conceptele de operații inteligente, câmp tactic inteligent sau războaie inteligente nu sunt noțiuni noi, acestea capătă noi conotații în contextul evoluției tehnologiilor în curs de dezvoltare.

Dezvoltarea infrastructurile militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G ne va permite să exploatăm mai bine celelalte tehnologii în curs de dezvoltare cum ar fi inteligența artificială, sistemele și dispozitivele autonome letale, stocarea datelor, roboții militari, biotehnologiile, sistemele hipersonice de lansare a rachetelor etc.

Pentru asigurarea unui spațiu cibernetic militar funcțional, normal și ultra securizat în condițiile implementării tehnologiilor de rețea 5G, propunem următoarele:

a) identificarea și implementarea unor arhitecturi integrate de securitate cibernetică bazate pe inteligență artificială;

b) dezvoltarea și integrarea comunicațiilor cuantice în infrastructurile militare operative de comunicații și tehnologia informației;

c) utilizarea tehnologiilor de criptare pentru fiecare dispozitiv conectat la rețea în câmpul de luptă;

d) permisivitatea accesării comunicațiilor satelitare la orice nivel tactic, operativ sau strategic de către orice dispozitiv securizat conectat la rețea.

În acest moment, nu putem afirma cu certitudine care tehnologie poate hotărî soarta unui conflict armat, însă un lucru este evident, anume faptul că inteligența artificială, spațiul cibernetic și infrastructurile militare operative de comunicații și tehnologia informației prin tehnologie de rețea 5G sunt elemente care contribuie semnificativ la redefinirea modului în care se vor desfășura viitoarele războaie inteligente.

Bibliografie:

1. BELLASIO, Jacobs, and SILVERSTEN, Erik, *The impact of new and emerging and technology on the cyber threat landscape and their implications for NATO, Cyber threats and NATO 2030: Scanning and analysis*, NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE, 2020.

2. KASKA, Kadri, BECKVARD, Henrik, and MINÁRIK, Tomáš, *Huawei, 5G and China as a Security Threat*, NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE, URL: https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/, 2019.

3. DASILVA, Luiz, H. REED, Jeffrey, SHETTY, Sachin, PARK, Jerry, WIJESEKERA, Duminda, WANG, Haining, *Securing 5G: NATO's Role in*

Collaborative Risk Assessment and Mitigation, NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE, URL: https://ccdcoe.org/uploads/2020/12/4-Securing-5G_ebook.pdf, 2020.

4. ***, Congressional Research Service, *Emerging Military Technologies: Background and Issues for Congress*, URL: https://fas.org/sgp/crs/natsec/R46458.pdf, 2020.

5. ***, *Threat assessment for the fifth generation of mobile telecommunications networks (5G)*, NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE, URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, 2019.

6. ***, Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: *Implementarea rețelelor 5G în condiții de siguranță în Uniunea Europeană – Punerea în aplicare a setului de instrumente al Uniunii Europene, Comisia Europeană*, Bruxelles, 29 ianuarie 2020.

7. ***, DOD *Announces $600 Million for 5G Experimentation and Testing at Five Installations, US Department of Defense*, 8 October 2020, URL: https://www.defense.gov/Newsroom/ Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati.

8. ***, *Post-Quantum Cryptography: Current state and quantum mitigation*, European Union Agency for Cybersecurity (ENISA), URL: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, 2021.

9. ***, *Security in 5G Specifications - Controls in 3GPP*, European Union Agency for Cybersecurity (ENISA), URL: https://www.enisa.europa.eu/publications/security-in-5g-specifications, 2021.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 917/2021

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro