ОСВРТ

УДК:355.01-51(73) : 004.7

МРЕЖНОЦЕНТРИЧНО РАТОВАNJE У ТЕОРИЈИ И ПРАКСИ ОС САД

Младен Костић, мајор

Мрежноцентрично ратовање (МЦР) нови је појам у теорији ратне вештине оружаних снага САД. Производ је информатичке ере у ратоводству, који, по мишљењу многих, суштински мења изглед рата и оружане борбе. Више пута долазило је до револуција у ратоводству, што је био одраз технолошког развоја (нпр. проналазак барута, парне машине, подморнице, авиона, радара, атомске бомбе и сл.). Међутим, неки аутори тврде да МЦР отвара нову епоху и да представља значајније откриће од барута.

Кључне речи: *трансформација одбране, кључни војни програми и технологије, мрежноцентрично ратовање.*

Увод

Индустријско друштво допринело је развитку човечанства развојем технике, технологије и људских ресурса који су многе снове људске цивилизације учиниле реалношћу. Истовремено, у достигнућа индустријског друштва спада и проналазак и коришћење наоружања високоубојног дејства и организација и употреба масовних војски које су употребљене у најкрвавијим и најдеструктивнијим ратовима у историји људске цивилизације.

Ново информатичко доба „невиђеном“ брзином мења индустријски свет, мада се информатичка ера базира на достигнућима индустријског друштва, па је тако проузроковало и суштинске промене у области ратоводства. Појава новог феномена глобалног тероризма и глобалне антитерористичке борбе после 9. септембра 2001, као и искуства из рата у Ираку 2003, потврђују да су савремени концепти ратовања, који су производ информатичке ере постали стварност. Нова стварност мења класичну слику ратишта 19. и 20. века и захтева нова промишљања.

Однос индустријске и информатичке ере у области ратоводства најбоље илуструје Ирачки рат из 2003, у којем су се сукобиле две војске које по битним обележјима припадају двема епохама.

Трансформација одбране САД и мрежноцентрично ратовање (МЦР)

Трансформација одбране[1] повлачи широку скалу несталних и прекиданих промена у наоружању, организацији и концепту извођења борбених дејстава, изазваних значајним променама технологије или појавом нових и различитих изазова међународне безбедности. Трансформација је неопходна да обезбеди оружаним снагама (ОС), као друштвеном организационом систему, континуитет деловања са позиција војне предности у подршци националних интереса.

Завршетком хладног рата и нестанка биполарне конфронтације са Совјетским Савезом, постављено је питање изгледа будућих снага и концепта њихове употребе, односно указала се потреба за њиховом трансформацијом. Ова активност на прилагођавању новим условима захватила је целе ОС САД, што је узроковало и промене у доктринама и организацији свих видова ОС САД.

Потпуно нови доктринарни приступ представљен је документом FM-1 (The Army) (објављен јуна 2001) као и новим борбеним правилом ФМ 3–0 (Operations), у којима се констатује да је доктрина КоВ-а САД на крају 20. века превазиђена, на шта указују слабости које су пратиле извођење операција након „Пустињске олује“, као што су операције у Сомалији, Босни, на Косову и Метохији, итд. Закључено је да сложена и нелинеарна природа војних операција захтева флексибилнију организацију бојишта, засновану на сврси, коју даје концепт „нелинеарне битке“.[2] Тиме је створена нова визија операција у које могу да се уклопе симултане и нелинеарне кампање, које се изводе у удаљеним зонама и на већој дубини него раније. Основна новина је стратегијска могућност реаговања, која не подразумева само брже распоређивање постојећих (формацијских) снага у простору, већ обухвата формирање, обуку, брзу дисперзију и истовремено ангажовање одговарајућих нових снага у време и на месту где су потребне. Команданту се тако омогућују опције за коришћење одлучујуће војне моћи, са новим садржајима и процедурама, а противнику, истовремено, стварају многобројне оперативне дилеме у нелинеарној сразмери. Копнене снаге се по новом концепту више оријентишу на циљеве који су им одређени и стварање адекватних способности од свих расположивих снага, а мање на географску повезаност (линеарни додир) са другим садејствујућим саставима. У знатно већој мери присутне су ваздушне, поморске и кампање специјалних снага.[3]

---

[1] R. O' Rurk: Defense transformation: Background and Oversight Issues for Congress, 9. 11. 2006, p. 3–5, www.fas.org/sgp/crs/natsec/RL32238.pdf

[2] R. Lopez: On Learning: Metric Based Systems for Countering Asymmetric Threats, School of Advanced Military Studies , United States Army Command and General Staff College, Fort Leavenworth, Kansas, p. 1–3.

[3] A. F. Krepinevich: Transforming the legions: the Army and the Future of Land Warfare, Center for Strategic and Budgetary Assessments, 2004, str. 12, www.csbaonline.org.

Сам концепт битке захтева софистицираније мере за постизање ефикасности. Разлог је, очекивано, врло сложено окружење у којем су информације у реалном времену капитална вредност. Због тога се у реализацији кампање тежиште ставља на команданта и проширује значај командовања у борби. Наглашава се потребна способност команданта и његових сарадника да на другачији начин представе, опишу, усмере, воде и стално процењују ток операција. То је условило да информационе технологије снажно утичу на нову концепцију рада команданта. Он сада, у потпуно новом (виртуелном) окружењу, планира и организује дејства, ствара визију борбеног простора и напада противника.

Становиште администрације САД јесте да Министарство одбране (МО) САД, трансформацијом, мора да постигне здружену, мрежноцентрализовано распоређену војну структуру, за супериорност у брзини доношења одлука. Да би постигло овај циљ МО гради доктрину, увежбава и наставља са градњом навика на континуалне промене које укључују: људе, процесе и системе.[4]

Појам мрежноцентричног ратовања

Мрежноцентрични прилаз ратовању је војно оличење концепта информатичког доба. Подразумева повезивање људи преко информационих токова, који почивају на интероперабилности система, рачунарима и комуникацијама, а користе их ОС САД. Укључује сарадњу и размену информација, обезбеђујући да се брзо остваре преимућства која ће командантима користити за време борбених дејстава. Овакво повезивање омогућава да се супериорност у информационим технологијама трансформише у борбену моћ.

Студије указују на то да умрежавање омогућава оружаним снагама да изведу различите врсте дејстава уз повећане борбене могућности у односу на неумрежене снаге, унапређивањем и ефикасности и делотворности извођења борбених дејстава (б/д).[5]

То се може уобличити у скуп циљева који се постижу увођењем МЦР:

1) самосинхронизација или иницијатива да се нешто уради без наређења;

2) унапређење схватања идеја „вишег“ командовања;

---

[4] C. Vilson, Network Centric Warfare: Background and Oversight Issues for Congress, 2. 6. 2004, p. 1, www.globalsecurity.org/military/library/report/crs/33858.pdf

[5] A. K. Cebrovski: The implementation of NCW, 5. 1. 2005, pp. 3–11, www.oft.osd/military/library_files/document_387/ncw_book_lowres.pdf

3) унапређење схватања оперативне ситуације на свим нивоима командовања;

4) повећање способности „утапања“ у заједничко знање целих ОС САД и савезника, да би се смањили магла и фрикција ратовања.[6]

Ако нови концепт и технологија буду доказани временом, улога МЦР, може се проширити и на стабилан фактор одвраћања у будућим сукобима. На пример, ако су противничке снаге неутралисане МЦР-ом пре него што су и ступиле у додир са ОС САД, борба може бити готова, пре него је и почела.

Развијене земље имају привремену предност, која ће се смањивати како се МЦР технологија буде ширила и на друге нације или терористичке групе. Ако желе да одрже предност САД морају наставити са усавршавањем употребе технологије да би се повећала флексибилност и прилагодљивост и за здружене и за савезничке операције, закључују водећи менаџери из области информационих технологија.[7]

Политиком подршке МЦР-у планира се повећање економске ефикасности елиминисањем застарелих система, подељених интереса, редундансе и неинтероперабилних система, као и оптимизацијом планирања инвестирања за постојеће и будуће информационе системе.

Кључни војни програми и технологија која омогућава МЦР

Да би се концепт МЦР-а реализовао неопходно је поседовање и развијање читаве гаме информационих технологија, које се ефикасно могу применити у војне сврхе.

Кључни војни програми

Министарство одбране САД одредило је следеће програме као кључне[8] за МЦР и за њих предвидело буџетске расходе по елементима за истраживање, развој, тестирање и оцењивање.

---

[6] Магла – непознавање ситуације; фрикција – неразумевање, одн. губљење нити идеје главнокомандујућег од стране потчињених.

[7] Закључци са годишње конференције Ц4ИСР у Меклену у Вирџинији, 6. маја 2004.

[8] C. Vilson: *исто,* стр. 15–20.

1) Централизација мреже

Овај програм намењен је подршци активностима информационе технологије за МЦР сарадњу. Хоризонтално спајање компоненти одређује како брзо програми МО и заједнице обавештајних служби могу бити проширени за МЦР оперативно окружење. Средства за еволуцију GIG[9]-а представљају компоненту, која тестира интероперабилност кључних система у маниру с краја на крај, укључујући Здружени тактички радио-систем (JTPC)[10] и програм глобалне мреже за повећање електронског опсега.

2) Глобална информативна мрежа МО (GIG)

Ова мрежа подржава активности и функције МО и заједнице обавештајних служби и омогућава размену информација између свих војних база, мобилних платформи и поседнутих положаја. Такође, GIG, обезбеђује одговарајући комуникациони интерфејс са савезницима, партнерима и онима који не користе мрежу МО САД. Старији информациони системи, као што су: систем порука одбране (ДМС),[11] ГЦЦС[12] и систем за глобалну борбену подршку, биће приступачни преко GIG -а.

Министарство одбране планира да опрема за војне везе до 2008. користи ИНТЕРНЕТ протокол 6 (Ипв6) као стандард за све трансмисије преко GIG. Нови ИПв6 протокол ће, наводно, нудити већу заштиту порука и боље праћење опреме, залиха и персонала, употребом дигиталних ознака.

Кључна архитектура мрежног сервиса за имплементацију GIG -а су: Air force C^2 constellation, Marine Corps Integrated Arhitecture Picture (MCIAP), Navy Force Net (NFN) i Army Land War Net (ALWN). Ова архитектура мреже постаће потпуно интероперабилна да помогне реализацију потпуног потенцијала МЦР-а.

3)Технологија РВ за напредно тактичко гађање (АТ3)[13]

Систем АТ3 комбинује информације сакупљене мрежом ваздухопловних сензора, ради идентификације тачне позиције непријатељевог система ПВО. Систем се заснива на координацији информација са различитих система на ваздухопловима.

---

[9] Global information grid – глобална информативна мрежа.

[10] Joint tactical radio system – заједнички тактички радио-систем.

[11] Defence message system – систем информација одбране.

[12] Global command and control system – глобални командно-контролни систем.

[13] Air Force Tactical Targeting Tehnology – технологија РВ за напредно тактичко гађање.

4)Веза 16 РВ (линк-16)

Тактичка веза података (TDL)[14] користи се у борби за размену информација између машина. Ови подаци су: радарски циљеви, информације о циљевима, статус платформи, слике и наређења. Сврха овог елемента програма јесте да обезбеди интероперабилност TDL РВ САД. Оружја, платформе и сензори у свим службама користе TDL, док други TDL укључују Линк 11, Situational Awar FY2 Data Link (SADL)i Variable Message Format (VMF).

5) Способност морнаричког кооперативног ангажовања (CEC)[15]

Систем CEC повезује бродове морнарице и ваздухоплове, који дејствују у одређеној зони у једну интегрисану ПВО мрежу, у којој се радарски подаци, прикупљени са сваке платформе, емитују у реалном времену за целу мрежу. Свака јединица у CEC мрежи спаја своје податке и податке прикупљене од других јединица. Као резултат, јединице у мрежи деле заједничку, константну слику у реалном времену за цео ПВО систем. Систем CEC дозволиће броду да отвори ватру ПВО на долазећи противбродски пројектил иако га не види, користећи радарске податке са другим јединицама у мрежи. Такође, биће могуће да се један пројектил ПВО са једног брода наводи са другог или то исто, али са авиона.

6)Армијска бригада и ниже јединице у командовању бојем 21 (FBCB2)[16]

Овај систем употребљен са компјутерском опремом „Трагач плавих снага“ основни је дигитални систем КоВ САД, који употребљава тактички ИНТЕРНЕТ за слање података са бојишта у реалном времену снагама на терену. За време операције „Ирачка слобода“ овај систем се користио на неким од БВП типа „бредли“ и на неким од тенкова М1А1 „абрамс“, као успешна замена за класичне карте и извештавање о сопственој позицији радио-везом. Компјутерска слика и могућности GPS-а омогућили су посади тенка

[14] Tactical Data Link – тактичка веза података.

[15] Cooperative engagement Capability – способност кооперативног ангажовања.

[16] Army Force XXI Battle Command Brigade and Below – армијска бригада и ниже јединице у командовању бојем.

да користи „Трагач плавих снага“ за одређивање локације, чак и усред ирачке пешчане олује, слично као што пилоти користе инструменте по лошем времену.

7) Здружени тактички радио-систем (JTRS)[17]

Министарство одбране одредило је да би систем војне радио-везе требало развити у сагласности са JTRS архитектуром, која обухвата заједничке, софтверски дефинисане, програмабилне радио-везе за мобилну комуникацију, укључујући и радио-везу способну за комуницирање преко сателита. Ново JTRS средство имаће тако направљене рутере да подржавају мрежу на бојишту са могућношћу за динамичко опорављање линија везе када год је рад једног или више чворова нарушен. Наводно постоје нека неслагања око тога да ли ће се војска одлучити за ласерску или JTRS везу преко радио-таласа на релацији свемир – земља. Тренутно, војне службе (родови) користе различите форме таласа, које тек треба да буду интероперабилне.

8) Здружени беспилотни ваздухопловни борбени системи (JUCAS)[18]

Овај програм комбинује претходне резултате постигнуте програмима борбених БЛ за РВ и морнарицу (DARPA) за заједничку архитектуру, ради постизања максималне интероперабилности.

Технологије које подржавају МЦР

Неки посматрачи изјављују да је цена уласка у МЦР операције конструисање мреже сензора. На пример ваздухоплови и друге платформе постају сензори када им се дâ способност комуникације и комбиновања информацијама, а многа оружја се више не разматра као обична муниција већ, такође, постају систем сензора, пошто се наводе на циљ док не експлодирају. Овај део разматра кључне компоненте МЦР система.

[17] Joint Tactica Radio System – здружени тактички радио-систем.

[18] Joint Unmanned Combat Air Systems – здружени беспилотни ваздухопловни борбени системи.

1) *Архитектура мреже*

Мрежноцентрично ратовање је високо зависно од интероперабилности комуникационе опреме, података и софтвера који омогућавају повезивање људи, сензора и платформи са људском посадом и без ње. Део МЦР технологије почива на радио-предаји, при оптичкој видљивости за микроталасе, ИЦ и ласерско зрачење. Други део повезује информације ради емитовања кроз ширу међумесну мрежу за глобалну расподелу преко оптичких каблова, микроталасних репетитора или заједно ниско и високо орбитних сателита. Дизајн ове технологије мора омогућити брзу комуникацију између појединаца у свим активностима и брзу размену података и информација између мобилних платформи и сензора који су у употреби у ОС САД. Архитектура, такође, мора да поседује могућност динамичког самооправка и реформирања мреже, када је нарушен један или више комуникационих чворова.

Вероватно су најпознатије војне мреже САД: Незаштићена интернет протокол рутер мрежа (NIPRNET) и Тајна интернет протокол рутер мрежа (SIPRNET). Архитектура ових мрежа издваја предају поверљивих SIPRNET порука из цивилног ИНТЕРНЕТА, док се велики проценат мање поверљивих NIPRNET порука прослеђује цивилним ИНТЕРНЕТОМ.[19] У прошлости су неке војне јединице наводно употребиле специјалну технологију енкрипције, која омогућава SIPRNET комуникацију преко NIPRNETA.[20]

2) *Сателити*

Сателити су круцијални део система који омогућава мобилну комуникацију у удаљеним подручјима, као и стварање слике о ратишту, навигацију, информације о времену, упозорење на пројектиле и способном да се преко њих шаљу захтеви назад до САД за додатну подршку. Глобални позициони систем (GPS) састоји се од 28 сателита, који помажу да се лоцирају снаге САД на терену, као и циљеви за оружје, као што су крстареће ракете. Сједињене Државе одржавају 6 орбиталних констелација за: извиђање, надзор и обавештајне активности (ISR). Како било, упркос великом броју војних сателита Агенција одбране за информационе системе (DISA) издала је саопштење да су комерцијални сателити обезбеђивали више од 84% сателитске комуникације за време операције „Ирачка слобода". Сателити МО нису могли да задовоље све војне захтеве за сателитску везу и зато је МО по-

[19] 70% NIPRNET порука се шаље преко ИНТЕРНЕТА.

[20] C. Vilson: *исто,* стр. 3–4.

стало једно од највећих муштерија комерцијалних сателитских сервиса. МО некада изнајмљује на лизинг сателитску везу преко DISA, а некада је заобилази куповином директно из привреде. Овакво обилажење може смањити интероперабилност и, по неким експертима, повећати редундансу.[21]

3) *Радио-веза*

Дигитализација комуникација (везе) кључни је елемент програма МО који је у вези са трансформацијом ОС САД. Дигитална технологија чини ефикаснијом употребу радио-везе него аналогна. Од 1991. захтеви за ширином радио-спектра драстично су нарасли због напора да се убрза саобраћај дигиталних информација. Званичници МО остају заокупљени питањем да ли ће обезбеђење електронских веза, преко система МО, моћи адекватно да прати нарасле војне захтеве и у будућности.[22]

4) *Возила без људске посаде (УВ)*

Возила без људске посаде – беспилотне летелице (UAV) , земаљска возила (UGV) и подводна возила (UUV) примарно се користе за извиђање. Међутим, њихове мисије еволуирају и у борбене. За време операције „Ирачка слобода“, приближно 16 „предатора“ и један „global houk“ били су у операцијама и даљински контролисани преко сателитског линка са командним местом у САД. Свако ово средство захтева широки таласни појас електромагнетног спектра за контролу и пренос извиђачких података, а служи и као релејно чвориште за МЦР мрежу.[23]

5) Компјутерски чипови

Закон Гордона Мура о интегралним колима предвиђа да се сваких 18 месеци компјутерски чипови тако развију да постану два пута сложенији и два пута бржи при истој цени, што значи да постају четири пута моћнији. Индустрија која користи компјутерску технологију почива на Муровом зако-

[21] *Исто*.
[22] *Исто*.
[23] *Исто*, стр. 4–5.

ну, као водичу за инвестирање у будуће технолошке системе. Многи будући концепти МЦР, које сада развија МО, почивају на еволуционом континуитету моћи компјутерског процесуирања и могу бити погођени напретком у другим технологијама, као што је нанотехнологија.[24]

6) *Нанотехнологија*

Нови материјали, развијени нанотехнологијом, могу евентуално променити ратну опрему на тешко замислив начин. Оружја могу постати мања и лакша, а нови минијатурни сензори мреже могу детектовати, лоцирати, идентификовати, пратити и нишанити потенцијалне претње, много ефикасније. Министарство одбране тренутно употребљава нанотехнологије да креира термоотпорне премазе који продужавају ресурсе погонским вратилима пропелера на ратним бродовима и као адитив за повећање перфомански ракетног погона.

Познаваоци верују да нанотехнологије могу изменити фундаменталне концепте ратовања, можда и више него барут. Према изјавама Лоа Цлифорда, истраживања која обавља Министарство одбране односиће се на све аспекте ратовања, оружја и комуникација, која користе војници.

У јуну 2003. Масачусетски институт за технологију (МИТ) основао је Институт за војне нанотехнологије у Кембрицу (САД). Институт је добио фонд од КоВ САД у износу 50.000.000 $ и почеће да развија технологије као што су: ручно средство за детекцију хемијског и биолошког оружја, флексибилан екоскелетон (непробојан прслук) који би смањио масу војничке опреме за 25 kg, док би се додали биомедицински сензори, повезани у мобилну мрежу. Друге земље, као што је Кина, такође, напредују у нанотехнологији[25]. У Азији је 2000. било 25.000 дипломираних стручњака у области нанотехнологије, док је у САД било нешто више од 5000.[26]

7) *Софтвер*

Софтвер је важна компонента свих комплексних одбрамбених система, коришћених у МЦР. Служба главног рачуноводства САД (ГАО) препоручила је МО да прати најбоље пословање фирми за софтвер у приватном сектору како би се избегло кашњење у распореду и прекорачењу трошко-

[24] *Исто*, стр. 5.

[25] Кинески научници су изузетно напредовали на овом пољу.

[26] C.Vilson,: *исто,* стр. 5.

ва, који су искомпликовали многе програме Пентагона, који зависе од сложеног софтвера. Многи верују да глобализација економије утиче на процесе софтверског развоја. У складу са тим, добављачи МО развој софтвера често поверавају мањим приватним фирмама, а у неким случајевима посао програмирања је повериван off-shore компанијама. То отвара полемику о могућности убацивања компјутерских вируса, односно малициозних програма, ради субверзије компјутерског система МО. Роберт Линц, директор одељења МО за информационо обезбеђење, наводно је изјавио да МО тренутно истражује начине да ојача политички механизам повећања поверења МО у безбедност страних и домаћих софтверских производа. Готово је немогуће наћи неовлашћен непријатељев програм унутар компјутерског програмског модула, који потиче из једне од многих земаља које производе софтвер.[27]

Примена МЦР технологија у недавним војним операцијама и вежбама

Операција „Ирачка слобода" пре би могла да се назове транзиционом него трансформационом, зато што се МЦР технологија није потпуно применила у свим јединицама, а неки делови система нису били довољно кориснички оријентисани. Неки познаваоци тврде да је МЦР концепт доказао ефикасност и потенцијал ратовања појачаног мрежом. Други верују да је тешко објективно интерпретирати искуство у примени МЦР, делом зато што процес сагледавања могу ометати они, који фаворизују трансформацију. Ипак, неки истичу да су последња искуства у примени МЦР-а обмањујућа јер су недавни противници били слаби и некомпетентни, укључујући Панаму (1990), Ирак (1991), СРЈ (1999) и Авганистан (2001). Неке традиционалне вредности војне моћи, каоште је доминација у ВаП-у, могу бити неоправдано умањиване. Према Лорену Б. Томсону, аналитичару Лексингтон института, у сагледавање претходних искустава може се претеривати у значају „здружености" и улоге специјалних операција. Ирачани су направили толико много грешака да се не би могло закључити да је њихов пораз узрокован вредношћу нове стратегије. Међутим, следећи пример говори у прилог тези да је примена нове МЦР технологије итекако имала утицаја.[28]

[27] *Исто*, стр. 6.

[28] A. K. Cebrovski: *исто,* стр. 27–31.

Искуства из рата у Ираку 2003.

Ирачка оклопна дивизија „Медина" је, 25. марта 2003, покушала да искористи јаку пешчану олују, која је требало да елиминише техничку супериорност противника и изврши противудар на 3. америчку дивизију у рејону прелаза преко реке Еуфрат у близини Наџифа. Међутим, 3. дивизију су подржале две летелица Global Hawk, које су летела јужно од Багдада и две или више летелице JSTARS, тако да је имала потпуни увид у ситуацију на војишту, упркос изузетно лошим метеоролошким условима. Захваљујући подацима који су се сливали у мрежу података и са оператерима на JSTARS, који су подацима обезбеђивали систем C4, америчка дивизија била је у стању да обезбеди прецизне податке за ваздухопловну и артиљеријско-ракетну подршку. Овај момент одлучујуће је допринео да бој буде решен у корист Американца и да оклопна дивизија од 10.000 људи са опремом вредном око милијарду долара, буде потпуно разбијена за два дана. Истовремено, америчка војска је, користећи ову надмоћ, успела да нанесе значајне губитке јаким ирачким снагама, које су са простора северно од Багдада биле упућене да подрже противудар дивизије Медина. Овај бој представљао је вероватно одлучујући моменат за сламање отпора ирачке војске.

Централна команда ОС САД 7. априла, 2003. је примила обавештајни податак од ЦИА-е, да је Садам Хусеин, са своја два сина и неколико сарадника из партије БААС договорио састанак у популарном ресторану у ексклузивном делу Багдада. За само пола сата зграда је лоцирана, напад одобрен и локализован GPS координатама са једног AWACS-а, а подаци прослеђени бомбардеру B-1B који је био у зони чекања. Дванаест минута касније зграда и бункер иза ње погођени су са четири бомбе JDAM од по 1000 kg. Због критично малог времена за реакцију, Садам и остали званичници успели су да избегну сигурно уништење, тако да је напад пропао, али је то било питање чисте среће или грешке дојаве, док је сама реакција система за сваку похвалу.[29]

Мрежне комуникације

Повећано умрежавање за време операције OIF, наводно, дозволило је ОС САД да развију много напредније могућности координирања брзог одређења циља. У операцији „Пустињска олуја" 1991. напори на координацији

[29] M. G. Vickers & R. C. Martinage: The Revolution in war, CSBA 2004, str. 7–69, www.csbaonline.org

одређивања циља захтевали су око четири дана. У операцији OIF, ОС САД смањиле су то време на око 45 мин. Априла 2003. у систем за командовање маринског корпуса слили су се подаци о искуствима при употреби неколико комуникацијских система за време борбених дејстава у Ираку. Неколико везиста, оперативних официра и команданата наводно су изјавили да су, углавном, били пренатрпани информацијама. Понекад је већина тих информација имала мало везе са циљем задатка. Примали су податке и слике са превише различитих мрежа, што је условљавало операсање великим бројем различитих модела комуникационе опреме. Неке јединице су у покрету или при изазовима комуницирања ван линије визирања често употребљавале E-mail и „чатовање“ за одржавање везе, што је обично тражило увезивање преко сателита.[30]

Сензори

Са „Трагачем плавих снага“ (BFT) FBCB2 су наводно добили читав низ похвала од јединица за помоћ у спречавању појаве савезничке ватре. BFT су портабл рачунари које преносе људи, возила и ваздухоплови, како би одредили своју стварну позицију преко GPS-а, а затим континуално емитовали те податке сателитском везом. Позиција сваке јединице затим се појављивала на командантским екранима осталих терминала BFT, као плава икона или на командним центрима. Кликтање на било коју плаву икону показивало би смер и брзину. Дупли клик је омогућавао текстуалну поруку директно до сваке јединице преко сателита.[31]

Сателити

Сателитска веза одиграла је кључну улогу у емитовању порука и слика за време OIF. Такође, омогућавала је везу са континенталним делом САД ради подршке. У сваком случају, растућа зависност од сателитских веза може постати критична тачка МЦР-а.

1) За време OIF, линије везе, укључујући сателитску везу, често су биле презасићене истовременим радом на свим доступним дигиталним фреквенцијама. Врх количине радио-преноса износио је 3 GB/S, што је било око 30 пута више него у Пустињској олуји 1991. Сателити МО нису могли да задово-

[30] C. Vilson: *исто,* стр. 23.

[31] *Исто*, стр. 24.

ље све војне захтеве, па је МО постало највећи појединачни корисник комерцијалних сателитских веза преко ДИСА, а некада и директном куповином из привреде. У сваком случају, то није добро, јер се обиласком ДИСА-е смањује интероперабилност између родова и служби, што повећава редундансу.

2) Комерцијални сателити употребљени су да допуне војне, који нису имали довољно капацитета, упркос чињеници да је већи број војних сателита померен на више геостационарне орбите и за Авганистан и за Ирак.[32]

Радио-таласи и смртоносност

Неки проблеми у каснијем стизању порука за време ОИФ могли су се десити због нерешених питања око руковођења и поделе радио-подручја. Некада су поруке са нижим приоритетом пажљиво одбациване ради слања других са вишим приоритетом.

1) Брзина којом су се трупе ОС САД кретале, поманкање сателитске везе и неспособност да се развуку оптичке везе онемогућили су напоре на повећавању опсега радио-везе. Повремено је од неких команданата тражено да деле један комуникациони канал, присиљавајући их да чекају на коришћење, када год је слободан.

2) Бригадни ниво командних места могао је користити сателитски поглед и слике у реалном времену са БЛ, али нижи нивои нису. Нижи нивои командовања су места где су, заправо, потребнији ситнији детаљи ради успешних дејстава.

3) Иако је КоВ САД уложио инвестиције на војном систему за подршку у доношењу одлука, неки од планова и колективних доношења одлука изведени су преко Е-маила и четовањем на које су војници навикли. Често су ови начини били доступни, када су други начини комуникације били недоступни, а уз то нису захтевали никакву додатну обуку.[33]

Ваздушна надмоћ

Беспилотне летелице могу носити термовизијске камере које могу видети по мраку или киши, што војним планерима улива самопоуздање при организовању напада. Међутим, без брзог успостављања превласти у ВаП-у,

[32] Исто, стр. 24–25.

[33] Исто, стр. 25–26.

БЛ и друга средства за обавештајно обезбеђење не би могла да се употребљавају за информације потребне систему МЦР. Беспилотне летелице и други ваздухоплови за подршку, као што су авио-цистерне, скоро су неодбрањиве, а њихова употреба дубље у ВаП-у Ирака била би скоро немогућа без превласти у ВаП-у.[34]

Операције са коалиционим снагама

Употреба МЦР технологије са коалиционим снагама резултирала је смањењем „пријатељске“ ватре за време ОИФ, када су коалициона средства оперисала као независни ентитети, а коалиционе снаге често су остајале ван планирања и извршавања, јер је већина информација слана преко система доступних само ОС САД. На пример, већина б/д у ВаП-у, која су претпостављала употребу технологије МЦР за коалиционе операције, ангажовале су само авијацију САД.

Политика размене поверљивих информација захтева одвојене уговоре између САД и коалиционих партнера. Министарство одбране тренутно одржава 84 одвојене обезбеђене мреже за МЦР коалиционе партнере (по једна за сваког партнера), јер национална политика разоткривања ограничава које се информације могу дати одређеним партнерима. Као прилог томе, и сваки коалициони партнер има своју одговарајућу политику за осетљиве информације. Резултат тога био је да су информације потребне за планирање операција биле ширене међу коалиционим снагама ручним путем, а трансфер података је заостајао за потребним вођењем операција. Једна сигурносна мрежа потребна је да ефикасно распоређује информације међу партнерима са могућношћу динамичког додавања и одузимања коалиционих партнера. У МО започет је програм назван „Мрежноцентрични подухват услуживања“ (NCES, такође познат као „Хоризонтална фузија“) како би информације биле доступне свим коалиционим партнерима, док би истовремено обезбеђивале снажну безбедносну заштиту преко мрежне енкрипције и контроле динамичког приступа. У сваком случају, ова техничка решења не треба да погађају различите заштитне политике поделе информација међу партнерима.[35]

---

[34] Исто.

[35] A.K.Cebrovski: *исто,* стр. 34–44.

Искуства из вежби ваздушне борбе

Предност технологија информатичког доба може се видети кроз неколико вежби вођених 1990. између ловаца британског краљевског ваздухопловства опремљених дата-линком са ознаком Линк-16 и класично навођених ловаца USAF. У читавој серији борби у ВаП-у показано је да је однос победа које су остварили британски према америчким ловцима био приближно 4 према 1. У читавом низу вежби које су касније извођене, а које су укључивале око 12.000 летова при ангажовању снага од 2 : 2 до 8 : 16, доказано је да је остварен 150% већи однос победа ловаца опремљених Линком-16 у односу на класично навођење. Слични резултати добијени су у вежбама између ловаца америчке морнарице против РВ, а чији су ловци били опремљени мрежном технологијом.[36]

Искуства из експеримената у америчком КоВ-у

Широк дијапазон експеримената која је предузела КоВ САД ради боље визуелизације бојишта резултирала је захтевом за изненађујуће повећаном количином муниције, чак пет пута већом него што је уобичајено. Разлог је био у затрпавању снага, које су учествовале у експерименту, броју информација и потенцијалних циљева и њиховом неселективном одабирању. То је узроковало повећано трошење муниције и коначно проузроковало промашај логистичке процене.

Овакав развој догађаја поновио се још неколико пута, с тим што се уочио и бржи утрошак муниције, а све то је имплицирало промену у смислу повећања, односно фокусирања логистике.[37]

Анализа предности и ограничења МЦР

Док САД имају могућност да експлоатишу предности процесуирања компјутерских информација, умрежавања, сателита, радио-комуникације и других технологија, неки познаваоци постављају питања да ли се војска САД

[36] C. Vilson: *исто,* стр. 33–35.

[37] A. K. Cebrovski: *исто,* стр. 50–52.

превише ослања на нанотехнологију и да ли је информација прецењена као војна предност.

Технологија је само једна од елемената МЦР-а. Други кажу да МЦР захтева промене у правилима понашања, процесима и организацији да би се превела предност информационог доба у борбену моћ. Кроз употребу МЦР технологије круте конструкције су трансформисане у динамичке и могу обезбедити нова и напредна прилагођавања за акције у борби. Понекад људи не схватају потпуне могућности нових система, јер се нису прилагодили новим условима.

Предности МЦР

Нова литература подржава теорију да се моћ интензивира деривацијом из информационе размене, приступа информацијама и брзини. Ово гледиште потврђује се резултатима из недавних ратних искустава, која показују да када су снаге стварно здружене, са обимно интегрисаним могућностима и када дејствују према принципима МЦР-а, оне могу потпуно да искористе високопоследичну природу информационог доба ратоводства. Мале промене у почетним условима резултирају енормним последицама.

Неке војне предности МЦР операција су следеће:

1) умрежене снаге састоје се од малих јединица које се могу кретати лакше и брже. То значи да неколико јединица са неколико платформи, носећи мало позадинског материјала, може извести ефикаснију или разноврснију мисију при мањим трошковима;

2) умрежене снаге могу користити нове тактике. За време операције „Ирачка слобода", КоВ САД је искористио покрет који се може описати као „тактика роја", јер је умрежавање дозволило војницима да прате једни друге и када нису у видљивом контакту. Снаге су могле да се крећу напред кроз Ирак, ширећи се у мале независне одреде (борбене групе), избегавајући „тесне" формације. Употребљавајући „тактику роја" састави су изводили кретање брзо, без обезбеђења позадине. Сви састави знали су међусобну локацију. Ако би један састав ушао у неприлике, други, у близини, брзо би дошао у помоћ и „којењем" би напали непријатеља сасређено из свих праваца. Из наведеног се могу донети следећи закључци:

– мање снаге са мало потребне опреме – вођење рата је јефтиније;

– теже је ефикасно напасти широко развучену формацију;

– борбене групе могу покрити више простора, јер не морају одржавати б/п ни успоравати због заосталих возила;

– познавање положаја властитих снага смањује могућност „пријатељске" ватре за време б/д;

– „ројење“ дозвољава напад директно у центар непријатељеве командне структуре, нарушавајући непријатељеву снагу изнутра, што је боље него борити се на линији додира на фронту;

3) начин на који појединац мисли и дела на бојном пољу такође се мења. Када јединица наиђе на тешке проблеме на терену јавља се Тактичком оперативном центру (ТОЦ), који класификује и разматра проблеме у соби за „чатовање“ (као на ИНТЕРНЕТ-у), употребљавајући Microsoft chat softwere. Проблем се решава „ројењем“ експерата, који могу бити размештени свуда и тако далеко као и Пентагон;

4) време откривања – гађања се скраћује. Употребљавајући МЦР системе, војник на терену има могућност да води анализу на „сајту“ рововских обавештајаца преко дисплеја сензора, што је боље него да чека повратну анализу из Пентагона. На пример, једна UAB са више сензора може осматрати исти рејон као десет стражара или може пратити рејон контаминиран РХБ агенсима, без ризика по људске животе. Данас МО има око 90 UAB, а до 2010. овај инвентар ће се учетворостручити.[38]

Прецењивање информација

Каже се да технологија информационог доба чини простор и време мање релевантним, а да информације повећавају корак догађаја и оперативни темпо ратовања. Неки експерти верују да умрежавање ради информационе размене није довољна замена за борбени маневар и да информатичка супериорност и праћење ситуације није најважнија компонента борбене моћи. Као у шаховској партији, знање следећег потеза је кључ успеха битке, нпр. кроз тачну анализу предвидети непријатељев потез и тактику.

По неким експертима, велики информациони ресурси су прецењени као предност у планирању б/д, а важне војне одлуке не морају бити донесене на информационо базираној рационалној анализи. Они тврде да је расправа о војној трансформацији превазиђено фокусирана на добицима од информација и да војне службе, представници за националну сигурност и заједница обавештајних служби нису темељно проучили опасности везане за доктрину зависну од података, што илуструју неки од погледа:

– квантитативне промене у информацијама и анализи често воде до квалитативне промене у појединачном и понашању целе организације, па су некада контрапродуктивне;

[38] C.Vilson: *исто,* стр. 7–8.

– поверење у софистициране информационе системе може одвести командовање у претерану самопоузданост;

– једно информативно богато окружење – богато могућностима, може променити вредност информацији, редефинисати циљеве и изазвати пораст могућности да се добију лоше последице.[39]

Потцењивање противника

Неки познаваоци верују да модел за МЦР МО можда потцењује непријатељеву способност да обмане сензоре или блокира информације потребне за МЦР. Једна од уочених слабих тачака јесте отворено публиковање планова употребе МЦР технологије у будућем рату. Управо као и за Мажино линију, пре Другог светског рата, непријатељ има довољно времена да испланира и избегне јаке и нападне слабе тачке.[40]

Интероперабилност

Поставља се питање да ли ОС САД могу постићи праву интероперабилност система и умрежавање између свих снага. Према изјавама, које је наводно дао генерал-мајор Мерилин Кваљоти (заменик директора DISA), још увек се развија застарео систем који пролази кроз структуру владе. Пример представља Глобални командни и контролни систем (GCCS), који ради под 16 различитих база података, што увећава архитектуру специјализовану за различита војна одељења и бранше. Наводно, DISA ће ускоро GCCS, верзију 4, испунити новом архитектуром, дизајнираном само за једну главну базу података.

Министарство одбране наводно намерава да интегрише мрежну архитектуру система, коју употребљавају све војне бранше, да би креирале могућност МЦР, повезаног са Глобалном информационом мрежом (GIG). Као помоћ овој интеграцији МО је направило нови Одбор са могућношћу присиле (FBC) да прати МЦР програм у вези са пропустима у финансирању или могућностима. Када се лоцира неки спор, FBC извештава здружено веће за преглед захтева (JROC), које обезбеђује информације за време дебате о буџету у Пентагону.[41]

[39] *Исто,* стр. 8–9.

[40] *Исто.*

[41] *Исто,* стр. 9–10.

Ограничења електро-магнетног спектра

Поставља се питање да ли радио-комуникације могу изаћи на крај са будућим војним потребама. Када радио-електронска подршка постане неадекватна за време борбе, команданти су, понекад, принуђени да одлучују о приоритету примопредаје порука. Они то чине привременим искључивањем неких радио и компјутерских уређаја, како би омогућили порукама са високим приоритетом да прођу. То одлаже или отказује друге поруке или примо-предају података који су класификовани са нижим приоритетом. Одлагање или отказивање ажурирања информација, због уског грла радиопредаје, може теоретски постићи да се нека јединице боре са опремом, а не са непријатељем или да непријатељ брже мења позицију него што информације стижу.

До 2010. Конгресна буџетска канцеларија очекује да користан фреквентни опсег радио-таласа у КоВ падне на ниво 1:10 у односу на захтевани. Према бившем помоћнику секретара одбране Полу Стенбиту, основна припрема за постизање интернет парадигме за МЦР јесте: наћи начин да се испуне захтеви за ширину фреквентног опсега радио-таласа. Комуникациона инфраструктура мора имати довољну ширину фреквенције електромагнетних таласа, нпр. да омогући да више људи на различитим локацијама на бојишту добије решење проблема преко компјутера у исто време, без ограничавања радио-таласног опсега.[42]

Предвиђање напретка хардвера до 2010. прошириће уска грла фреквентног опсега са бригадног на корпусни ниво. Ако се здружени тактички радио-систем (JTRC) буде показао као према пројекту КоВ-а, моћи ће да обезбеди довољну ширину за ниже тактичке нивое командовања, са могућношћу даљег раста, према захтевима после 2010. Углавном, за дивизијски и корпусни ниво пројектовани захтеви биће већи него што се, вероватно, могу задовољити.[43]

Космичка доминација

Сједињене Америчке Државе у великом мери зависе од космичке доминације у комуникационим, извиђачким, метеоролошким и системима за рано упозорење на лансирање пројектила. Имале су космичку доминацију у прошлом заливском рату, јер противници нису експлоатисали свемир, нити

[42] У одређеним ситуацијама неки команданти имају само један комуникациони канал. Ако неко почне да га користи пре командант остаје на чекању.

[43] *Исто,* стр. 10.

су угрожавали космичке системе САД. Међутим, САД се не могу ослањати на исту предност у будућности и могу очекивати да технолошки мање напредне нације и ваннационални субјекти примене електронско ометање или нападну земаљске сателитске станице. Недржавни субјекти би, такође, могли остварити предност космичке технологије, изнајмљивањем сателитских фреквенција или извиђачких сателита са опремом високе резолуције која долази из Русије, Кине или од других носилаца космичких програма.

Сателити ће се у будућности користити за космички базиране радаре (СБР), који ће обезбеђивати сталан поглед на бојно поље, укључујући и добијање тачних података о терену, ради мапирања. Међутим, унутар обавештајне заједнице расте сумња за дужу употребу сателита у улози ISR платформе у будућности. Како непријатељ постаје другачији и више неконвецијалан, може почети да користи различите технологије, као што су оптички каблови, који су изван домашаја сателитских сензора. Три констелације сателита користе се за прислушкивање непријатељевих радио, мобилних и микроталасних емисија. Две констелације 6 сателита користи се за извиђање и слање слика у видљивом, ИЦ и радио-фреквентном подручју.[44]

Набавке из других извора и трансфер технологије

Пораст набавке преко off-shore компанија високотехнолошких послова, укључујући и програмирање и производњу микрочипова, може омогућити трансфер технологије и евентуално угрозити глобалну технолошку супериорност САД и нарушити тренутне предности МЦР технологије. Потврда ове чињенице је да је од 2027 доктората на универзитетима у САД у 2003. години 63% било неамеричке националности, а од 15 906 магистара – 56% су странци. Истраживачка фирма Гарднер група открила је да ће корпорацијска потрошња на готове услуге информационих технологија порасти са 1,8 милијарди $ у 2003. на 26 у 2007, а пола од тог посла отпада на азијске земље, као што су Индија и Кина.

Прављење уговора за националну одбрану спада међу најтеже набавке из других извора, којима се бави савезна влада. Унутар МО однос приватног сектора и јавног је скоро 5:1 и даље расте у корист приватног. Док набавка може бити мотивисана смањењем трошкова, нови тренд за послове истраживања и развоја на високом нивоу јесте да се ради на off-shore принципу, делимично и због раста образовања и талента међу страним радницима. На пример у 1998. Intel Co., microsoft Co. и др. ИТ фирме отвориле су погоне за истаживање и развој у Пекингу и другим деловима Азије.

[44] *Исто,* стр. 10–11.

Трансфер технологије такође се дешава у производњи опреме високе технологије, која се употребљава за МЦР операције. На пример, само 20% термалних батерија, које се користе за пројектиле, вођену артиљерију и вођене бомбе произведене су у САД, док су остале набављене од страних добављача. ИЦ средства за осматрање ноћу, која су недавно давала знатну војну предност, сада се производе од материјала и компоненти које су готово у целости из страних извора.

Недавна студија МО закључује да коришћење страних компанија, као извора набавке високо-технолошке опреме, не погађа дугорочно борбену готовост, а за већину високотехнолошких производа неколико домаћих произвођача је способно да испуне потребе МО. Као додатак томе, неки познаваоци верују да компаније у САД, које се баве производњом високе технологије морају задржати флексибилност и да усагласе своје послове са потребама тржишта. На пример, у складу са порастом вештина страних произвођача да производе квалитетно, купци високо-технолошке опреме предност ће давати нижој цени, а не техничком таленту. Компаније које игноришу тренд набавке чине то на штету дугорочне компететивности.[45]

Асиметричне претње за супротстављање МЦР

Термин „асиметричан“ односи се на стратешко у ратовању и често се описује као напад слабијег или слабије опремљеног непријатеља када спозна слабе стране јачег непријатеља. Технологија је обезбедила дисиметричну предност САД у прошлим сукобима. Међутим, дисиметрично некад води до непредвиђених последица. Снимци који показују ненадмашну моћ војне силе САД у недавним урбаним сукобима приказани су на светским медијима. Такав имиџ снаге, проистекао из ефикасности ОС САД, могу дати терористичким организацијама, као што је Ал Каида, додатну реторичку моћ, могућност регрутовања нових чланова и постизање праве лојалности.

Асиметричне контрамере укључују активности непријатеља да заобиђу МЦР сензоре или да негирају корисност високотехнолошког оружја. Неке методе могу укључивати: бомбаше самоубице; нерегуларне борце и снајперисте малог домета да остваре сасређен напад и брзо нестану; мешање непријатељевих снага са цивилима као штитом; употребу бомби за ширење нуклеарног материјала или отпада; хемијско и биолошко оружје.

Особе придружене терористичким групама могу имати напредно образовање из области високе технологије и могу знати како да то знање употребе

[45] *Исто,* стр. 11–12.

у асиметричном нападу на инфраструктуру МЦР. На пример Калид Шеик Мухамед, који је ухапшен 2003. због могућих веза са Ал Каидом, наводно је студирао машинство на универзитету С. Каролина. Неколико терориста који се доводе у везу са догађајима од 11. септембра такође је имало дипломе из високог образовања у области високе технологије.

Могући начини асиметричног напада на МЦР су:

– управљани напад енергетским средством ради ометања сателитских сигнала;[46]

– управљана енергетска средства, која теоретски могу да спрже електронска кола компјутера са дистанце;[47]

– компјутерски вируси који нарушавају контроле комплексних оружја.[48]

Сајбер напад на војне компјутере

Министарство одбране САД предузело је кораке на блокирању неких комуникационих портова који повезују NIPRNET са цивилним ИНТЕРНЕТОМ. Међутим, у октобру 2003. цивилни хакер је привремено заузео NIPRNETОВ wеб сајт. Други хакери такође су користили цивилни ИНТЕРНЕТ за инфилтрацију на војне компјутере, правећи одређену штету и присиљавајући на привремено искључење војне мреже.

Расте контроверза о томе да ли ОС САД треба да користе „отворене изворе“, односно компјутере за опште комерцијалне сврхе у напредним системима за тенкове, авионе и другу сложену опрему. На пример „LINUX“ је означен као „отворен извор“, јер га је развијала светска заједница програмера, који су у континуитету додавали нове ствари, допуњавајући једни друге и јавно размењујући изворе. Мора се напоменути да термин „отворен извор“ има различито значење и да некада „затворен извор“, као што је Microsoft Windows, због права о власништву, у ствари није сасвим затворен за јавност.

NSA је истражила сигурне верзије LINUX-а, али није јасно да ли су сви војни компјутери ограничени резултатима тих истраживања. Неки експерти верују да софтвер са слободног тржишта нарушава све принципе безбедности и да могу бити заражени непријатељевим вирусима, као што је тзв. „тројанац“, који може проузроковати да цео систем не функционише. Са друге

[46] Група Иранаца је наводно ометала комерцијалну сателитску везу проревпоуционарним порукама читаве две недеље са станица на Куби.

[47] На пример високоенергетско микроталасно средство активирано хемијским експлозивом. Као такво, наводи се портабл верзија, величине актовке, са специјално обликованом антеном, која би могла да створи пулс енергије у одређеном смеру на даљини од 1 km.

[48] C. Vilson: *исто,* стр. 12–14.

стране, има потпуно супротних мишљења, по којима је ЛИНУХ тешко компромитовати од неке агенције, будући да је потпуно отворен и доступан широкој заједници програмера широм света, који га усавршавају и дограђују.

У недавној студији DISA констатује се да МО тренутно користи знатну мешавину софтвера, виталну за информациону сигурност МО. То је делимично зато што су многи заштитни програми, које користи МО, израђени коришћењем свима доступног софтвера, а ефектни дупликати нису доступни из „затворених извора", производа недоступних јавности. Студија потврђује да би wеб сервис МО и развој софтвера МО био прекинут без сталног коришћења свима доступног софтвера, јер су алати (већина програма) на којима почива wеб дизајн и развој софтвера базирани на широко доступном софтверу.

Експерти са морнаричке КШШ[49] наводно су изјавили да „субверзија софтвером" може бити избегнута употребом софтвера високе сигурности, који је доказано „чист" од малициозних вируса. Због додатног ригорозног развоја и тестирања, овакав софтвер би коштао знатно више од тржишних.[50]

Закључак

Мрежноцентрично ратовање је концепт информационе супериорности извођења операција којим САД организују своје снаге и воде б/д у информатичком добу. На основу искустава из борбених дејстава која су водиле ОС САД намеће се закључак да ће умрежене снаге потући оне које то нису, иако су у свему осталом једнаке. Подаци и информације о могућностима МЦР, сакупљене кроз широки дијапазон дејстава и активности ОС САД (б/д, вежбе, експерименте итд.), генеришу неколико главних чињеница, односно ставова који се намећу о МЦР:

– добро умрежене снаге побољшавају размену информација, али и квалитет информација, јер, условно речено, до невиђених размера унапређују командо-информациони систем;

– размена података о ситуацији омогућава садејство и самосинхронизацију и повећава непрекидност и ефикасност командовања, као и брзину доношења одлука и њиховог спровођења. То у крајњем случају повећава темпо извођења операција;

– све то драматично увећава ефикасност извршења задатка и постизање циља борбеним дејствима. Мрежноцентрично ратовање претаче информациону

[49] Након израде новог заштитног алата на Морнаричкој постдипломској школи, за заштиту од неауторизованог упада у компјутрске системе, нова технологија је лиценцно продата цивилној компанији. То је учињено јер се сматра да ће комерцијална употреба програма омогућити даљи развој и усавршавање.

[50] C. Vilson: *исто,* стр. 14–15.

супериорност у борбену моћ, ефикасним повезивањем савезничких снага на бојишту, знатним увећањем знања о ситуацији, што „убрзава“ командовање, повећава ватрене могућности снага на бојишту и могућност преживљавања.

Као нови извор борбене моћи, МЦР знатно утиче на планирање и вођење операција, омогућавајући ОС САД да уђу унутар противниковог циклуса одлучивања, мењајући и диктирајући темпо извођења борбених дејстава. Само заиста здружене снаге, са свеобухватно интегрисаним могућностима и дејствујући по принципима МЦР-а, могу експлоатисати бенефиције информатичког доба. Оне то чине мењајући почетне борбене услове, одржавањем високог степена промене и сталним креирањем нових борбених услова, који онемогућавају да противник реагује ефикасно.

Брзина је критична за успех концепта превентивног одвраћања – брзина развоја, организације, ангажовања и подршке. Способност да се одлучи и делује брже од противника, како би се омогућило постављање или мењање услова и одређивање повољног тренутка, једном речју да се оствари потребна брзина – могућа је умрежавањем.

Без обзира на поменуте недостатке и проблеме при употреби МЦР, предности су очигледне, што значи да ће се овај концепт само даље развијати. То упућује на размишљање о трансформацији наших ОС и њиховом организовању и опремању у складу са будућим трендовима.

Литература

1. R. O’ Rurk: Defense transformation: Background and Oversight Issues for Congress, 9.11.2006, www.fas. org/sgp/crs/natsec/RL32238.pdf

2. R. Lopez: On Learning: Metric Based Systems for Countering Asymmetric Threats, School of Advanced Military Studies, United States Army Command - and General Staff College, Fort Leavenworth, Kansas, 2006. www.storming-media. us/45/4540/A454054.html

3. C. Vilson: Network Centric Warfare: Background and Oversight Issues for Congress, 2. 6. 2004.

4. A. K.Cebrovski; The implementation of NCW, 5.1.2005, www.oft. osd/military/library_files/document_387/ncw_book_lowres. pdf

5. M. G.Vickers & R. C.Martinage: The Revolution in war, CSBA 2004, www.csbaonline. org

6. C. Vilson: Network Centric Operations: Bacground and Oversight Issues for Congress, 15. 3. 2007,www.fas. org/sgp/crs/natsec/RL32411

7. A. F. Krepinevich: Transforming the legions: the Army and the Future of Land Warfare, Center for Strategic and Budgetary Assessments, 2004, www.csbaonline. org