Nerijus Maliukevičius*
Vilniaus universiteto Tarptautinių santykių ir politikos mokslų institutas

Karinis konfliktas informacijos amžiuje ir Lietuvos pasirengimas

Informacinė revoliucija keičia tarptautinę sistemą ir saugumo aplinką, kurioje mes gyvename. Valstybė praranda galios monopolį globalioje informacinėje erdvėje. Tačiau tos pačios technologijos tampa ir naujo tipo karinių konfliktų įrankiais. Griūna Vakarų civilizacijos suvokimas apie karinį konfliktą: anksčiau remtasi Carl von Clausewitz modeliu, kai vadovai iškelia politinius tikslus ir kontroliuoja karius, kariai tiesiogiai kariauja ir yra teisėti smurto taikiniai, civiliai nedalyvauja konflikte, bet remia savo vadovus per mokesčių sistemą bei palaiko jų iškeltus politinius tikslus. Informacijos amžiaus konfliktas – tai tam tikra prasme ikivestfalinis konfliktas, kai nusikaltimai prieš civilius ir valstybės vidaus tvarką buvo norma.

Kyla klausimas – kaip valstybė gali užtikrinti savo piliečių saugumą? Didžiosios valstybės atsakymą bando rasti sudarant informacinių operacijų strategijas ir programas. Didelis dėmesys čia skiriamas valstybės viešajai informacijai konflikto metu bei informacijos saugumui. Pastarojoje srityje Lietuva jau žengė pirmuosius žingsnius, tačiau viešosios informacijos principų – ne tik karinio konflikto, bet ir taikos metu – mūsų valstybei derėtų pasimokyti.

Įvadas

Kariniai konfliktai – tai neatsiejami tarptautinės sistemos raidos, jos kaitos elementai. Dėl tarpvalstybinių karų kisdavo teritorijų priklausomybė, įsitvirtindavo naujos tarptautinių santykių normos: laimėtojams užtikrinamas palankus *status–quo*, atsirasdavo naujų tarptautinių organizacijų, tarptautinių režimų. Tačiau toks santykis visada buvo abipusis: tarptautinėje sistemoje vykstantys procesai lemdavo karinio konflikto pobūdį, potencialius jo dalyvius, naudojamas priemones.

Vienas esminių globalių procesų, kuris prasidėjo gerokai anksčiau, nei baigėsi Šaltasis karas, yra informacinė revoliucija. Ji paveikė kiekvieną žmogų, kasdienę jo veiklą, ekonomines, visuomenines ar kitokias institucijas ir, svarbiausia, kiekvieną valstybę, jos vaidmenį tarptautinėje arenoje. Teigiama, kad po industrinės revoliucijos arba po branduolinio amžiaus, kurie buvo praeito amžiaus varomosios jėgos, prasideda informacijos amžius. Tarptautiniuose santykiuose formuojasi globali informacinė erdvė, kur komunikacijos priemonės ir informacinės technologijos panaikina laiko ir erdvės ribas. Taigi keičiasi tarptautinė sistema, formuojasi nauja saugumo aplinka, drauge keičiasi ir karinių konfliktų pobūdis.

XX amžiaus pabaigoje ypač sumažėjo informacijos surinkimo, skleidimo bei efektyvaus naudojimo kaštai. Tai įvyko dėl sparčios informacinių technologijų rai-

[*] *Nerijus Maliukevičius* - Vilniaus universiteto Tarptautinių santykių ir politikos mokslų instituto doktorantas. Adresas: Vokiečių 10, 01130 Vilnius, tel. 8-5-2514130,
e-paštas: n.maliukevicius@vilsat.net.

dos. Todėl nenuostabu, kad šiuo metu daugelis valstybių, įskaitant ir Lietuvą, plėtoja informacinės visuomenės, žinių visuomenės, elektroninės vyriausybės ir pan. programas, nes savo gerovę sieja su efektyviu informacijos panaudojimu.

Teigiama, kad „informacija – tai ne tik gamybos, bet ir griovimo pagrindas“[1]. Informacinė revoliucija paveikė konfliktą, kuris gali vykti įvairiais lygiais. Rusijoje dažnai aptariami informaciniai karai tarp oligarchų ar politikų, o tokios valstybės, kaip JAV, Kanada, Rusija ar Kinija, vysto informacinių operacijų programas ar strategijas, su kuriomis sieja savo valstybės saugumą arba dalyvavimą ateities kariniuose konfliktuose.

Šiame straipsnyje siekiama pažvelgti, kokią įtaką informacinė revoliucija padarė karinio konflikto pobūdžiui, kaip ateities konfliktai suvokiami JAV ir NATO, kokiomis priemonėmis šios organizacijos užtikrins savo saugumą. Siekiama pažvelgti, ko Lietuva galėtų pasimokyti iš šių karinių galios centrų.

Naują požiūrį į karinį konfliktą apibendrina informacinių operacijų samprata*, kuri straipsnyje bus apžvelgta išsamiau. Lietuva netrukus taps NATO nare, mūsų šalis konfliktų Afganistane ir Irake metu buvo suteikusi galimybę JAV ir kitoms NATO sąjungininkėms prireikus naudotis Lietuvos oro erdve ir oro uostais. Be to, Lietuva pasiuntė savo karininką į JAV karinių pajėgų vadavietę (CENTCOM), o šalies specialiųjų pajėgų kariai, karo medikai, krovinių gabenimo specialistai dalyvauja realiose karinėse operacijose. Nepaisant to, susidaro įspūdis, kad Lietuvos politikai, karo ekspertai miglotai suvokia informacinį karą, informacines operacijas bei informacinį saugumą, kaip šie reiškiniai lemia priimamus politinius ar karinius sprendimus. Matyt, daroma prielaida, kad informacinės operacijos ar gynyba nuo jų – tai didžiųjų bei turtingųjų valstybių prerogatyva. Tačiau tokia prielaida yra klaidinga ir tai įrodo Austrijos pavyzdys, kuris bus pristatytas straipsnyje.

Taigi šio straipsnio tikslas nėra bandyti įrodyti, kad Lietuva turėtų kurti analogišką JAV informacinių operacijų strategiją ir tam mesti didžiulius finansinius resursus,– tai netikslinga, nes tapusi NATO nare ji perims šios gynybinės sąjungos analogiškų operacijų patirtį ir standartus. Priešingai, tikslas – atskleisti, ką šioje sferoje yra pasiekusios JAV, NATO ir ką Lietuva turėtų perimti spręsdama savo valstybės administravimo bei politikos klausimus. Informacinių technologijų saugumo užtikrinimo sferoje mūsų valstybė jau žengia pirmuosius žingsnius – patvirtinta Informacinių technologijų saugos valstybinė strategija bei jos įgyvendinimo priemonių planas. Tuo tarpu dabartinė valstybės viešosios informacijos politika yra nekoordinuota – potencialaus karinio konflikto metu mūsų valstybė susidurtų su ypatingais sunkumais. Todėl būtina pasinaudoti NATO patirtimi šioje sferoje.

1. Informacinė revoliucija ir tarptautinė sistema

Daugelis autorių, bandančių apibendrinti tarptautinės sistemos vaizdą po Šaltojo karo, daro išlygą, kad dešimtmetis – tai per mažas laiko tarpas, norint konstatuoti, kad jau nusistovėjo vienokia ar kitokia šios sistemos būsena. Populiaru pateikti

---

[1] Baylis J., Smith S., eds., *The Globalization of World Politics*, Oxford University Press, 1997, p. 554.

* Kartais vartojamas informacinio karo terminas, tačiau oficialiuose JAV ir NATO dokumentuose vartojama informacinių operacijų sąvoka.

keletą scenarijų: pvz., Huntington, Fukujamos, kapitalistinės sistemos pergalės, Pax Amerikana ir pan. scenarijai. Ian Clark manymu, kol tarptautinių santykių disciplinoje ir pačioje tarptautinėje sistemoje vyrauja chaosas, šį laikotarpį teisingiausia būtų apibūdinti kaip „naujos istorinės epochos pradžią, kurios dominuojantis tarptautinių santykių faktorius yra fragmentacija“[2]. Autorius tokią išvadą prieina dėl dviejų priežasčių: visų pirma kartu su Šaltuoju karu baigėsi sisteminės priešpriešos tarp kapitalistinio ir komunistinio polių laikotarpis, antra, ši sisteminė priešprieša neutralizavo arba vieno iš polių naudai pajungė visas kitas etnines, nacionalines, religines aspiracijas. Žlugus bipolei sistemai, visos šios jėgos tapo nebekontroliuojamos. Todėl Ian Clark teigia, kad pagrindinis tarptautinių santykių ekspertų uždavinys šiuo metu yra nustatyti naujas konflikto ašis, o jų, skirtingai nei Šaltojo karo metu, gali būti keletas[3]. Tokiame kontekste ypač svarbu išsiaiškinti, koks yra modernios valstybės vaidmuo garantuojant savo piliečių saugumą.

Daugelis autorių pabrėžia, kad nyksta valstybės suvereniteto reikšmė tarptautiniuose santykiuose, t. y. daroma prielaida, kad valstybė praranda galios monopolį. Didžia dalimi tai sąlygojo informacinė revoliucija – valstybė prarado monopolį į informaciją. Šį procesą pradėjo M. Thatcher ir R. Reagan telekomunikacijų revoliucija[4]. Taigi prasidėjo globalus telekomunikacijų sektoriaus dereguliacijos procesas*, dėl to tarptautinėje arenoje išaugo telekomunikacijų korporacijų reikšmė. John Baylis ir Steve Smith teigia, kad informacinė revoliucija tarptautinės sistemos dalyviams turėjo nemažą įtaką.[5] Pirma, vis daugiau informacijos yra prieinama valstybėms ir kitiems tarptautinių santykių dalyviams, tačiau tai turi teigiamą poveikį tik tada, jei sugebama šią informaciją efektyviai apdoroti ir panaudoti, priešingu atveju iškyla informacijos pertekliaus problema. Antra, globalūs informacijos kanalai leidžia decentralizuoti valdymą, tuo naudojasi transnacionalinės korporacijos, tarptautinės organizacijos, net teroristinės grupuotės, tuo tarpu valstybės valdymas yra paremtas centralizuotu sprendimų priėmimo mechanizmu, todėl šioje srityje valstybė susiduria su rimtais sunkumais. Trečia, nebėra informacijos kontrolės monopolio, todėl išauga žiniasklaidos, ypač pasaulinių televizijos kompanijų, vaidmuo. Ketvirta, informacinė revoliucija pasireiškia globaliu skaidrumu, t. y. problemos, kurios anksčiau buvo laikomos valstybių vidaus reikalu, tampa globaliomis problemomis, ir tai tik pagilina valstybės suvereniteto eroziją. M. E. Olsen ir M. N. Marger teigia, kad žiniasklaida, kuri yra pagrindinė informacijos formuotoja ir skleidėja, dėl informacinės revoliucijos tapo viena iš pagrindinių galios institucijų tarptautinėje sistemoje[6].

Tačiau reikia atsižvelgti ir į tai, kad informacinė revoliucija valstybėms suteikia ir tam tikrų galimybių. Globaliame pasaulyje valstybė gali įtvirtinti savo galią ne vien kariniu ar ekonominiu potencialu, bet ir komunikacija grindžiama kultūros

---

[2] Clark I., *Globalization and Fragmentation: International Relations in The Twentieth Century*, Oxford University Press, 1997, p. 172.
[3] *Ten pat*, p. 174.
[4] John Baylis, Steve Smith., eds., (note 1) p. 542.
* 1981 m. priimtas Britanijos telekomunikacijų įstatymas, 1984 m. suskaidyta JAV telekomunikacijų monopolistė AT&T.
[5] John Baylis, Steve Smith, eds., (note 1) p. 549.
[6] Olsen M. E., Marger M. N., eds., P*ower in Modern Societies*, Westview Press, 1993, p. 238.

sklaida. H. H. Frederick valstybes, vykdančias tokią politiką ir taip išnaudojančias savo galią, vadina hegemonais[7]. Tai labai suprastintas sąvokos vartojimas, tačiau šiuo atveju ji puikiai apibūdina JAV politiką po Šaltojo karo.

2. Informacijos revoliucija ir konfliktas

Taigi valstybė, siekdama piliečių saugumo, turi prisitaikyti prie globalios informacinės aplinkos ir drauge keistis. Visos modernios kariuomenės investuoja dideles lėšas į komunikacijų ir informacinių technologijų sektorių. Kinta karo technologija ir strategija. Skirtingas strategijas JAV karo ekspertai palygina tokiomis schemomis:

INDUSTRIJOS AMŽIUS INFORMACIJOS AMŽIUS

1 schema. Industrijos ir informacijos amžių karo strategijų piramidės[8]

Globalioje informacinėje erdvėje vykstančių modernių karinių konfliktų metu lemiamą reikšmę turi informacijos kontrolė bei efektyvus ją lemiančių priemonių taikymas.

Dabar vykstantį paradigminį pokytį galima palyginti su tuo, kuris vyko po Vestfalijos sutarties. Prieš Trisdešimties metų karą nebuvo aiškaus skirtumo tarp karinės kampanijos ir masinio banditizmo. Richard Mansbach ir Edward Rhodes teigia, kad Vestfalijos sutartimi Europos valstybių lyderiai nusprendė apriboti karą, ir tai nulėmė ateities karinių konfliktų pobūdį[9]. Nuo to laiko pradėta skirti, kas yra „legitimus“ kariavimas – vykdomas profesionalių karių prieš kitus karius, siekiant konkrečių valstybių vadovų iškeltų politinių tikslų, ir kas yra „nelegitimus“ kariavimas – nusikaltimai prieš civilius ir valstybės vidaus tvarką. Taigi „kariauja tam tikrai valdžiai (suvereniai valstybei) atsakinga individų grupė (profesionalūs kariai) ir remiamasi aiškiai apibrėžtomis taisyklėmis, ribojančiomis smurto naudojimą“[10]. Smur-

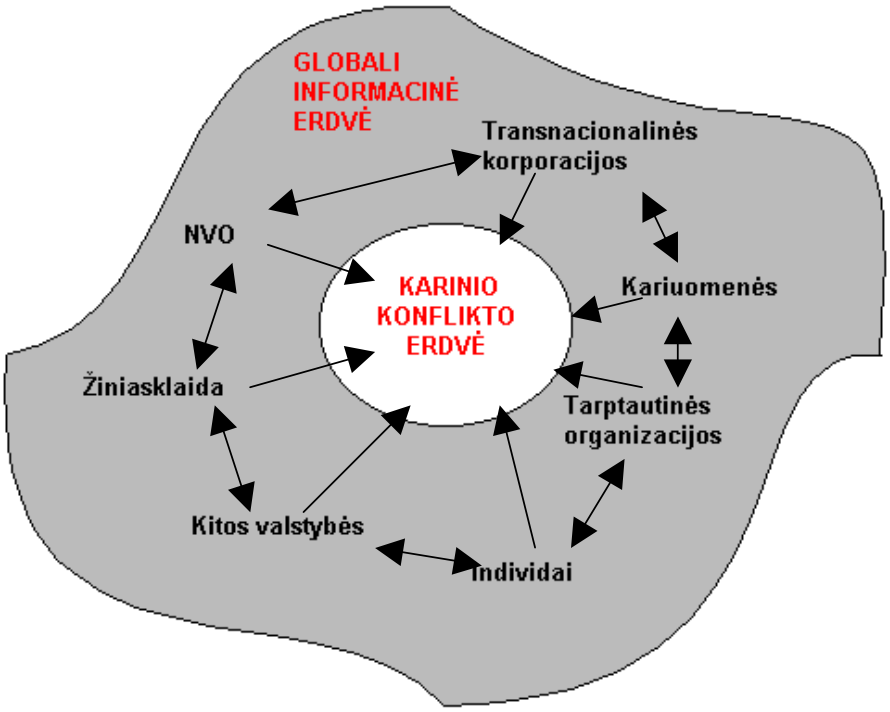
[7] Frederick H. H., *Global Communication and International Relations*, Belmont: Wadsworth Publishing Company, 1992, p. 205.
[8] Report of the Defence Science Board Task Force on Information Warefare – Defence. – Defense Science Board, 1996. http://cryptome.org/iwdmain.htm 06 09 2003.
[9] Mansbach R., Rhodes E., eds., *Global Politics in a Changing World*, Boston: Houghton Mifflin, 2003, p. 35.
[10] *Ten pat*, p. 35.

tas tapo dar viena politikos priemone, kurią galėjo naudoti Europos valstybių monarchai, kai kitomis priemonėmis nepavykdavo pasiekti norimų tikslų. Tokia kontroliuojamo smurto samprata tapo Prūsijos karininko Clausewitz teorijos apie karą pagrindu. Šio karininko teiginys apie karą kaip politiką, vykdomą kitomis priemonėmis, bei jo sukurta karo trikampio samprata suformavo Vakarų civilizacijos suvokimą apie karinį konfliktą. Tačiau dabar šis suvokimas sparčiai kinta ir panašu, kad grįžtama prie ikivestfalinės karinio konflikto sampratos: nusikaltimai prieš civilius ir valstybės vidaus tvarką tampa norma.

Prielaidos pokyčiams atsirado daug anksčiau. Clausewitz teorijoje karo trikampio kampuose atsiduria šie trys veiksniai: vadovai iškelia politinius tikslus ir kontroliuoja karius, kariai tiesiogiai kariauja ir yra teisėti smurto taikiniai, civiliai nedalyvauja konflikte, bet remia savo vadovus mokesčiais bei palaiko jų iškeltus politinius tikslus. Šis karininkas suformulavo riboto, arba kontroliuojamo, karo sampratą. Tačiau I ir II Pasauliniai karai, Richard Mansbach ir Edward Rhodes manymu, pademonstravo, kaip karinės technologijos pokyčiai, galimybė mobilizuoti visos valstybės ekonomiką karo reikalams bei išplitęs nacionalizmas gali sugriauti šį teorinį trikampį[11]. Pasauliniai karai buvo totalūs, kur nebuvo daromas skirtumas tarp karių ir civilių, o valstybių vadovai labai sunkiai kontroliavo konflikto procesus. Šaltojo karo metu karinė technologija buvo toliau vystoma, ir JAV, ir Sovietų Sąjunga sukūrė branduolinį ginklą. Šaltajam karui pritaikius Clausewitz teoriją, galima teigti, kad karas tarp supervalstybių tapo neįmanomas, nes, vykdomas kitomis priemonėmis, jis nebūtų racionalios politikos pavyzdys. Tačiau riboti kariniai konfliktai šiuo laikotarpiu vyko, pavyzdžiui, Vietname, Afganistane. Po Šaltojo karo karinė technologija toliau vystėsi neįtikėtinais tempais, tačiau karinį konfliktą Persijos įlankoje Lawrence Freedman ir Efraim Karsh dar priskiria ribotų karų tipui[12], kuriems pritaikoma Clausewitz karo trikampio samprata: JAV vadovybė turėjo aiškų politinį tikslą – išvyti Irako armiją iš Kuveito; šį įvykdžius, Prezidento G. W. Bush administracija kito tikslo – nuversti Sadamą Huseiną – nebekėlė; koalicijos vykdomi tiksliniai smūgiai gali būti Clausewitz akcentuojamo aiškaus karių ir civilių atskyrimo iliustracija; be to, ne tik JAV visuomenė, bet ir tarptautinė bendruomenė palaikė koalicijos veiksmus ir buvo tuo trečiuoju ramsčiu.

[11] *Ten pat*, p. 35.
[12] *Ten pat*, p. 49.

Tačiau šis konfliktas jau vyko naujoje aplinkoje, kurią JAV, Kanados, NATO karo ekspertai vadina globalia informacine erdve:



2 schema. Karinio konflikto vieta globalioje informacinėje erdvėje[13]

Globali informacinė erdvė – tai institucijos, organizacijos, sistemos, esančios už karinio konflikto ribų, tačiau galinčios daryti įtaką pačiam konfliktui. Anksčiau šią erdvę išskirtinai kontroliavo valstybės, tačiau informacijos amžiuje reikšmingas gali būti kiekvienas tarptautinių santykių subjektas, jo intencijos ir veiksmai. R. Garigue ir T. Romet teigia, kad „visi procesai vyksta globalioje informacinėje erdvėje, o ji daro tiesioginę įtaką šiems procesams“[14]. Pati įtakingiausia veikėja šioje erdvėje yra žiniasklaida, kuri karinių konfliktų metu „gali paveikti strategines kryptis bei karinių operacijų apimtį“[15], tačiau ne mažiau įtakingos gali būti nevyriausybinės organizacijos, transnacionalinės organizacijos, tarptautinės organizacijos, individai, kitos valstybės ar jų kariuomenės, jei jos sugeba efektyviai kontroliuoti informaciją globalioje informacinėje erdvėje. Praeitame dešimtmetyje šioje erdvėje dominavo tokios

[13] Garigue R., Romet T., „Information Warfare and the Canadian Forces“, *National defense, May 1996.* http://www.iwar.org.uk/iwar/resources/canada/iw_&_cf.pdf 06 09 2003.
[14] *Ten pat.*
[15] *Ten pat.*

tarptautinės žiniasklaidos korporacijos, kaip CNN, BBC, tačiau dabar į šias pozicijas pretenduoja islamo kultūrą ir vertybes propaguojantys Al–Jazeera, Al–Arabia televizijos kanalai. Kokį svarbų vaidmenį televizija vaidina globalioje informacinėje erdvėje, parodo ir J. Chirac iniciatyva steigti prancūziškąjį CNN analogą: „Tai teisėtas mūsų šalies siekis, ir aš norėčiau, kad jis būtų įgyvendintas; Prancūzija turi aktyviau dalyvauti filmuotos medžiagos kovoje, kuri vyksta tarp pasaulio televizijų“[16].

Šioje globalioje aplinkoje išauga teroristinių, radikalių religinių ar panašių organizacijų reikšmė, o jų veiksmai konflikto metu griauna iki tol vyravusį Clausewitz modelį. John Keegan teigia, kad informacijos amžiuje bus būdingi postmodernūs konfliktai ir valstybė turi būti pasiruošusi juos spręsti: „Postmodernaus karo samprata griauna suvokimą, kad karai vyksta tarp suverenių valstybių, kai smurtu siekiama įtvirtinti vienos valstybės politinę valią prieš kitą“[17]. Nauja konflikto samprata atspindi valstybės suvereniteto, politinės valdžios fragmentacijos tendenciją. Karas nebėra tik valstybių politika, vykdoma kitomis priemonėmis, – tai gali būti teroristų „politika“. Gerokai mažėja galimybės kontroliuoti konfliktą – anksčiau už tai atsakingos būdavo konflikte dalyvaujančios valstybės. Postmodernus konfliktas nebetenkina ir kitų Clausewitz karo trikampio sampratos teiginių: nebelieka aiškaus skyrimo tarp karių ir civilių, keičiasi ir jų vaidmuo konflikto metu. Į tarptautinius karinius konfliktus įsitraukiant teroristinėms organizacijoms ar radikalioms religinėms grupuotėms, smurto vykdytojai tampa tarsi beasmeniai „tarptautiniai teroristai“. Be to, civilius jie pasirenka kaip „legitimius“ karinius taikinius. Kinta ir šių grupių vaidmuo konflikto metu. Pirma, konflikte dalyvaujančių pusių politiniai tikslai nebėra tokie aiškūs arba jų neįmanoma kontroliuoti, pavyzdžiui, jei tarptautinių teroristų tikslas yra kova su JAV ir visa Vakarų civilizacija, iškyla klausimas, kaip ir kada šis tikslas bus pasiektas. Antra, konflikto metu Clausewitz civiliams priskyrė materialios ir ideologinės paramos savo valstybei vaidmenį, tačiau informacinė revoliucija pasireiškia globaliu skaidrumu, todėl esmine problema tampa vidaus ir tarptautinės paramos politiniams bei kariniams tikslams garantavimas. Čia galima pateikti ir Lietuvos pavyzdį karo Irake metu, kai mūsų šalies televizijos žiūrovai galėjo stebėti karo veiksmus ne tik per tarptautinius CNN ar BBC televizijos kanalus, bet ir per Al–Jazeera, kurią retransliavo TV3 kanalas[18].

3. Valstybės vaidmuo užtikrinant savo piliečių saugumą informaciniame amžiuje

Taigi naujame tarptautinių santykių ir saugumo kontekste valstybės peržiūri savo pasirengimą dalyvauti naujo tipo kariniuose konfliktuose, analizuoja priemones, kuriomis būtų užtikrinamas savo piliečių saugumas. Andriu Latham mano, kad „šiuo metu vyksta karo reikalų revoliucija, kai industrinį totalų karą (I ir II Pasauli-

[16] J. Chirac siūlo įsteigti ištisą parą transliuojantį pasaulinį žinių kanalą. http://www.delfi.lt/archive/index.php?id=1784033 06 09 2003.
[17] Mansbach R., Rhodes E., (note 9) p. 59.
[18] TV3 transliuos „Al–Jazeera“ kanalo medžiagą, http://www.delfi.lt/archive/index.php?id=2085167 06 09 2003.

niai karai) keičia toks karas, kurį galima pavadinti įvairiai: informacijos karas, tikslinių smūgių karas, kibernetinis karas[19]. Tokį paradigminį pokytį lemia keletas faktorių: tobulėjanti karo technologija, ypač tai, kas susiję su informacijos revoliucija; naujų technologijų dėka mažėjanti masinė armija*; be to, po Šaltojo karo besiformuojanti nauja, bet grėsmę kelianti saugumo aplinka. Tačiau ne mažiau svarbi yra JAV – šios revoliucijos flagmano – tradicija naujas koncepcijas įtraukti į taktinius, strateginius dokumentus – doktrinas. Todėl tai apima ne tik teorinius apmąstymus apie būsimus konfliktus, bet ir praktinį kariuomenės parengimą dalyvauti juose.

Andriu Latham teigia, kad karo istorija yra paženklinta revoliuciniais pokyčiais: patrankos/parako, Napoleono karų, industrinio totalaus karo ir pan. revoliucijos. Kai kurie autoriai skiria iki dešimties tokių revoliucinių etapų, kiti, kaip Alvin Toffler, šneka apie tris revoliucines karų bangas: ikiindustrinę, industrinę ir informacinę[20]. Dupuy, remdamasis greičio ir technologijos kaitos santykiu, teigia, kad egzistuoja keturi periodai, o rusų generolas ir teoretikas Slipchenko mano, kad Persijos įlankos kare buvo naudojami šeštos kartos ginklai[21]. Tačiau svarbiau išsiaiškinti ne tai, kuri periodizacija yra tiksliausia, o tai, kodėl dabartiniai karo reikalų pokyčiai yra laikomi revoliuciniais. Martin Show teigia, kad praeito amžiaus kariniai konfliktai buvo totalūs dėl dviejų priežasčių: pirma, konflikto metu valstybės pagrindinį dėmesį skyrė totaliam griovimui; antra, šie konfliktai išsiskyrė totalia visuomenės ir valstybės ekonomikos karo reikalų mobilizacija [22]. Pažvelgus į konfliktus Persijos įlankoje, Kosove, Afganistane ir Irake, į akis krenta tikslinis, o ne totalus griovimo pobūdis. Be to, vidaus ir tarptautinių karo veiksmų palaikymas yra vienas esminių konflikto sėkmės garantų, o tam reikia didžiulių pastangų – daug didesnių nei totalių karų metu. Andriu Latham mano[23], kad karo pokyčius derėtų laikyti revoliuciniais dėl trijų priežasčių: informacinė revoliucija pakeitė informacijos surinkimą, saugą, perdavimą ir pristatymą, t. y. šio proceso greitis artėja prie nulinės ribos, o tai leidžia kalbėti apie virtualų karo lauko vaizdą – suprantama, kad keičiasi sprendimų priėmimo kariuomenėje procesas iš hierarchinio į decentralizuotesnį. Be to, masinį griovimą keičia tikslinis griovimas, o tai sąlygoja masinės armijos mažėjimą, t. y. atsiranda profesionalių, specializuotų pajėgų poreikis. Trečioji priežastis – grėsmių diskurso evoliucija, t. y. išnykus JAV ir Sovietų Sąjungos priešpriešai atsiranda jau minėtos naujos konflikto ašys.

JAV armijos Operacijų ir planavimo Departamentui priklausantis Strateginių Studijų institutas savo tyrime „Karinis konfliktas XXI amžiuje: informacinė revoliucija ir postmodernus karas“ teigia, kad kariuomenė šiuo metu turi būti ypač savikritiška ir tuo pat metu įvertinti pokyčius, vykstančius globaliame versle: „Šiandien

---

[19] Latham A., „Re–imagining Warfare: The „Revolution in Military Affairs“ // Snyder C.A. ed., Contemporary Security and Strategy, New York: Routledge, 1997, p. 210.

* Lietuvos kariuomenės reformos planai taip pat numato nuo 20 tūkst. iki 7 tūkst. mažinti karinį rezervą, taip pat turėtų mažėti savanorių skaičius – Lietuvos kariuomenė persitvarkys kolektyvinei gynybai, http://www.delfi.lt/archive/index.php?id=1869108 06 09 2003.

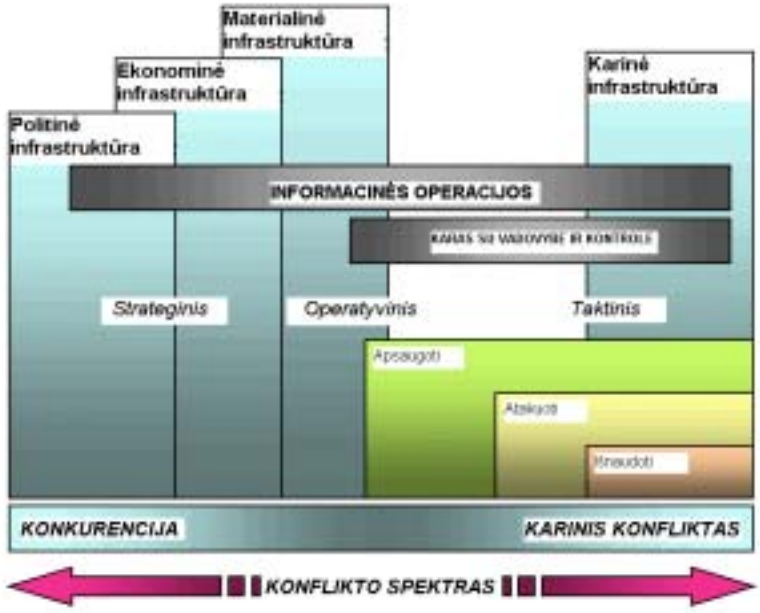
[20] Toffler A., *War and anti–war: Survival at the Dawn of the Twenty–first Century*, 1993, p. 301.

[21] Bosch J. M. J., „Information Operations: Some Operational Reflections“ in Bosch J. M. J., Luiijf H. A. M., Mollema A.R., eds., *Information Operations, NLARMS*, 1999, p. 80.

[22] Latham A., (note 19) p. 216.

[23] Latham A., (note 19) p. 220.

sėkmingai ir efektyviai verslo organizacijai būdingas globalus požiūris į verslą, decentralizuotą valdymą, strateginės partnerystės tinklą visame pasaulyje bei lankstumą priimant svarbiausius sprendimus“[24]. Atitinkami pokyčiai turėtų vykti ir karinėje srityje. Kaip jau minėta, informacijos amžiuje svarbiausias faktorius yra efektyvi informacijos kontrolė, todėl JAV Gynybos departamentas yra įsitikinęs, kad šalies kariuomenė ateities kariniuose konfliktuose turi siekti informacijos dominavimo[25]. Ši nuostata įtvirtinta Vieningoje Informacinių operacijų doktrinoje. Anot J. M. J. Bossch, „informacinės operacijos lemia ne tik karinę sferą – jos daro poveikį nacionaliniams, tarptautiniams ir globaliems politikos, ekonomikos sluoksniams, taip pat valstybėms, sąjungoms bei tarptautinėms visuomenėms“[26] ir jos gali būti naudojamos įvairiose konflikto spektro stadijose.



3 schema. Informacinių operacijų vaidmuo konflikto spektre[27]

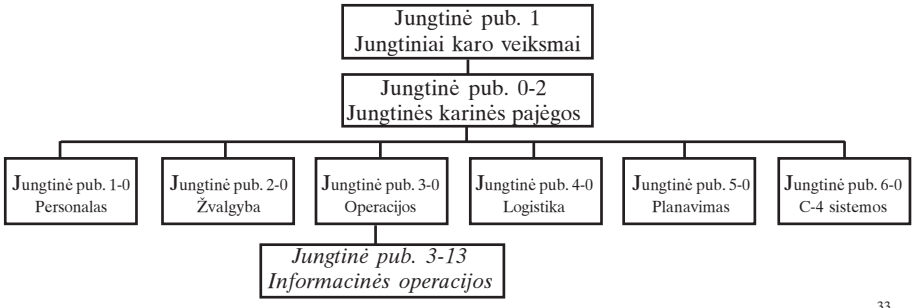
[24] Metz S., *Armed Conflict in the 21st Century: the Information Revolution and Post–modern Warfare*, Strategic Studies Institute, 2000, p. vii.
[25] *Ten pat* , p. x.
[26] Bosch J. M. J., (note 21) p. 79.
[27] Information Warfare Architecture, http://www.herolibrary.org/iwarch.htm 06 09 2003.

4. JAV požiūris į informacines operacijas

Informacinių operacijų samprata oficialiuose JAV dokumentuose pirmą kartą atsirado 1992 m. gruodžio mėn., kai Gynybos departamentas patvirtino 36.00.1 direktyvą, kur informacinės operacijos taip apibrėžiamos: „Tai į globalią informacinę erdvę nukreipti kariniai veiksmai, kuriais siekiama paveikti priešininko informacines arba sprendimo priėmimo galimybes“[28]. Šis apibrėžimas evoliucionavo ir 1998 m. spalio 9 d. patvirtintoje Vieningoje informacinių operacijų doktrinoje pateikiama paskutinė jo versija: „Informacinės operacijos – tai veiksmai, kuriais siekiama paveikti priešininko informaciją ar informacines sistemas, drauge apsaugant savo informaciją ir informacines sistemas“[29]. Pabrėžtina, kad ir Rusija 2000 m. patvirtintoje karinėje doktrinoje į informacines operacijas žvelgia taip pat kaip ir JAV: „Informacinės operacijos – informacinės (informacinės techninės bei informacinės psichologinės) atakos, nukreiptos prieš Rusiją ar jos sąjungininkes“[30]. Tais pačiais metais patvirtinus Rusijos Informacinio saugumo doktriną, buvo siekiama apsaugoti Rusiją nuo potencialių informacinių atakų.

JAV Vieningoje informacinių operacijų doktrinoje pabrėžiama, kad informacinių operacijų naudojimas konflikto metu yra „esminė sąlyga, norint pasiekti iškeltus uždavinius“[31]. Doktrina numato, kad minėtos priemonės turi būti taikomos tiek strateginiame, tiek operatyviniame, tiek taktiniame lygiuose, nepriklausomai nuo konflikto intensyvumo: ir karinėse operacijose ne karo metu, ir krizėse, ir pačiame kare[32]. Taigi šie veiksmai apima visą konflikto spektrą, kuris buvo pristatytas 3 schemoje. Dokumentas apima puolamąsias ir gynybines informacines operacijas, jų definicijas, naudojimo organizavimą bei vadovavimą. Be to, dalis dokumento yra skiriama informacinių operacijų planavimo metodologijai, koordinavimo principams, nemažai dėmesio skiriama apmokymams, pratyboms ir modeliavimui. JAV Vieningą informacinių operacijų doktriną derėtų laikyti išsamiausiu ir esminiu kariniu dokumentu, skirtu šiai naujai ateities karinių konfliktų sferai.

Vieningų doktrinų hierarchija



4 schema. Informacinių operacijų doktrinos vieta vieningų JAV doktrinų hierarchijoje[33]

[28] Bosch J. M. J., (note 21) p. 91.
[29] *Joint Doctrine for Information Operation*s, 1998, www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf 06 09 2003.
[30] Военная доктрина Российской Федерации. – Совет Безопасности Российской Федерации, 2000 04 21, http://www.scrf.gov.ru/Documents/Decree/2000/706–1.html 06 09 2003.
[31] *Joint Doctrine for Information Operations*, (note 28) p. vii.
[32] *Ten pat*, p. II–7.
[33] *Ten pat,* p. GL–11.

Doktrinoje puolamosios informacinės operacijos, t. y. „veiksmai, kuriais siekiama paveikti priešininko informaciją ar informacines sistemas“, apima operatyvinį saugumą, karinį nuslėpimą, psichologines operacijas, elektroninį karą, fizines atakas – griovimą, specialias informacines operacijas* . Gynybinės informacinės operacijos, t. y. „veiksmai, kuriais siekiama apsaugoti savo informaciją ar informacines sistemas“, apima informacijos užtikrinimą, operatyvinį saugumą, fizinį saugumą, kontrnuslėpimą, kontrpropagandą, kontržvalgybą, elektroninį karą ir specialias informacines operacijas.

Doktrinoje vadovavimo informacinėms operacijoms funkcija suteikiama Jungtinės vadovybės pirmininkui, kuris „yra pagrindinis Gynybos sekretoriaus patarėjas informacinių operacijų klausimais, tvirtina šių operacijų planus, užtikrina nuolatines informacinių operacijų pratybas ir karinio personalo mokymus“[34] . Karo vadai „atsako už tiesioginį informacinių operacijų planavimą, vykdymą ir pratybas“[35] . Karinio konflikto metu informacinių operacijų planavimas ir modeliavimas yra patikimas informacinių operacijų ląstelei. Pabrėžtina, kad doktrina numato ateityje reorganizuoti egzistuojančią vadovavimo ir kontrolės ląstelę į informacinių operacijų ląstelę[36] . Taigi informacinės operacijos JAV ateityje taps karinės strategijos pagrindu. Jos savyje sujungs vadovavimo ir kontrolės funkcijas.

Strateginiame lygyje doktrina numato, kad „bus imtasi veiksmų, kuriais bandoma paveikti visus priešininko galios elementus (karinį, politinį, ekonominį bei informacinį), drauge apsaugant savo ir sąjungininkų galios elementus“[37] . Operatyviniame lygyje informacinės operacijos naudojamos kariniams kampanijos tikslams pasiekti, o taktiniame jos naudojamos konkretiems, kartais specifiniams taktiniams tikslams įgyvendinti[38] . Doktrinoje yra išdėstyti principai, kuriais remiantis turi būti vykdomos informacinės operacijos: pirma, pagrindinis šių operacijų taikinys – priešininko sprendimų priėmimo procesas; antra, informacinių operacijų tikslai turi būti aiškūs ir suderinti su nacionaliniais interesais bei bendrais kariniais tikslais; trečia, puolamosios priemonės turi būti parenkamos pagal priešininko pajėgumą bei jo atsako galimybes; ketvirta, iš anksto turi būti nustatyta, ar informacinės operacijos yra centrinės, pagalbinės, ar tik dalinės puolamosios karinės priemonės; penkta, šios operacijos turi būti visiškai integruotos į visus JAV karinius veiksmus[39] . Atkreiptinas dėmesys į doktrinos teiginį, jog strateginiame lygyje informacinės operacijos turi būti paremtos viešosios informacijos kampanija ir glaudžiu bendradarbiavimu su civilinėmis institucijomis bei organizacijomis. Doktrinoje teigiama, – ir tai itin svarbu,– kad informacinių operacijų sėkmę nulems karinės ir civilinės sferos informacinių veiksmų derinimas. JAV už viešąją informaciją atsako Valstybės departamentas, kuris šias funkcijas centralizavo panaikinus JAV Informacijos agentūrą. Tai turėtų tapti pavyzdžiu Lietuvai, kur, reiktų pripažinti, dažnai atskirų Vyriausybės institucijų ar net ministerijų viešosios informacijos veiksmai yra nesuderinti. Karinio konflikto metu toks nesuderinamumas būtų pragaištingas.

* Doktrinoje neatskleidžiamas jų turinys.

[34] *Ten pat,* p. I–6.

[35] *Ten pat,* p. I–6.

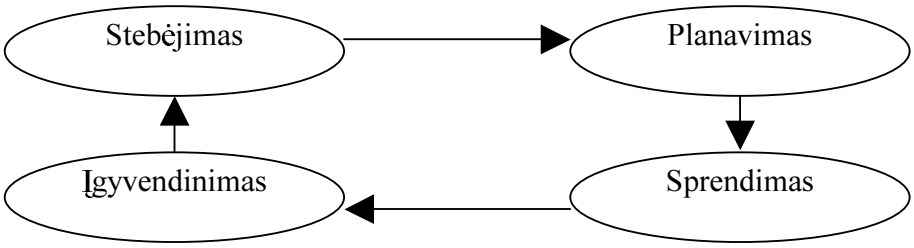
[36] *Ten pat*, p. ix.

[37] *Ten pat,* p. I–2.

[38] *Ten pat,* p. I–3.

[39] *Ten pat,* p. II–1.

Informacinių operacijų taikiniai gali būti labai įvairūs: vadovybė (civilinė, karinė, socialinė, kultūrinė ir pan.), civilinė infrastruktūra (telekomunikacijos, transportas, energija, finansai, gamyba ir pan.), karinė infrastruktūra (komunikacijos, žvalgyba, logistika ir pan.), karinės sistemos (lėktuvai, laivai, artilerija, tikslinė ginkluotė, priešlėktuvinė gynyba ir pan.). Visų šių struktūrų efektyvų funkcionavimą užtikrina technika, todėl ji tampa pagrindiniu taikiniu. Tačiau kadangi technika tėra priemonė tam tikriems veiksmams atlikti, tikruoju taikiniu visada išliks žmogaus protas, o tiksliau – sprendimų priėmimo mechanizmas*.



5 schema. Sprendimo priėmimo mechanizmas[40]

Atsižvelgiant į tai, doktrinoje ypatingas dėmesys yra skiriamas informacinių operacijų gynybai: operatyvinio saugumo priemonės turi nustatyti pažeidžiamiausią informaciją ar informacines sistemas ir sukurti jų apsaugos mechanizmus; elektroninio karo priemonės turi prisidėti prie šios apsaugos funkcijos; švietimas ir pratybos turi diegti karinio ir civilinio personalo suvokimą apie informacinį saugumą, nes didžioji informacijos nutekėjimo dalis – tai žmogiškojo faktoriaus pasekmė; žvalgyba ir kontržvalgyba turi analizuoti ir nustatyti grėsmes; kontrnuslėpimas turi klaidinti priešininką ir nukreipti jo puolamąsias pastangas kita linkme; kontrpropaganda turi atskleisti priešininko psichologines operacijas. Gynyba turėtų apimti keturis etapus: informacinės aplinkos apsaugą; atakos šaltinio nustatymą; funkcijų atstatymą ir atsaką į ataką. Doktrinoje informacinė aplinka – tai nacionalinė informacinė infrastruktūra, susidedanti iš privataus, vyriausybės ir gynybos sektorių. Rusijos Valstybinės tarnybos akademijos Nacionalinio saugumo katedros vedėjo pavaduotojas A. V. Vozženikov pabrėžia, kad „vieninga nacionalinė informacinė infrastruktūra bus naudojama kaip efektyvus resursas, tačiau dėl to jis taps potencialiu taikiniu“[41]. Tad jos apsauga – tai esminė sąlyga. Be to, apsauga yra ir santykinai pigiausia lyginant su kitų trijų gynybos etapų (atakos šaltinio nustatymo, funkcijų atstatymo, atsako) kaštais. Todėl būtent šioje srityje Lietuva turi perimti jau sukauptą patirtį, ypatingą dėmesį atkreipiant į mažesnių valstybių, tokių kaip Austrija, pasiekimus, kurie bus aptarti vėliau.

* Šį terminą įtvirtino JAV Oro pajėgų generolas John Boyd.

[40] US Information Operations Field Manual FM 100–6. – Headquarters Department of the Army, Washington, DC, 27 August 1996, http://www.atsc–army.org/cgi–bin/atdl.dll/query/download/FM/100–6/fm100–6.zip 06 09 2003.

[41] Колесникова Е. Что век грядущий нам готовит?, http://www.nosorog.com/public/safety/prognoz.html 06 09 2003.

5. NATO požiūris į informacines operacijas

Tiek karinėse NATO operacijose, tiek karo strategijos reikaluose JAV visada užėmė lyderio vaidmenį. Todėl nestebina tai, kad NATO požiūris į informacines operacijas yra beveik identiškas išdėstytam JAV Vieningoje Informacinių operacijų doktrinoje. 1999 m. sausio 22 d. Šiaurės Atlanto Taryba patvirtino NATO informacinių operacijų strategiją. Šis dokumentas nuo JAV doktrinos skiriasi tuo, kad ypatingą dėmesį sutelkia į strateginius veiksmus (tai atsispindi pateikiamame informacinių operacijų apibrėžime): „Strateginiai yra tokie veiksmai, kuriais, siekiant politinių ir karinių tikslų, daroma įtaka sprendimų priėmėjams, paveikiant priešininko informaciją ir informacinius procesus, vadovavimo ir kontrolės galimybes, drauge apsaugant savąsias“[42]. Šis apibrėžimas, skirtingai nei JAV suformuluotas, nėra pritaikytas tik karinei sferai. Čia kalbama apie poveikį sprendimo priėmėjams nepriskiriant jų nei kariniams, nei politiniams, nei verslo ar kt. lyderiams, t. y. NATO informacinės operacijos yra orientuotos į strateginį lygmenį, kur siekiama užsitikrinti paramą savo veiksmams konflikto metu ir tuo pat metu palaužti priešininko valią. Jose Gardeta teigia, kad „strateginiame lygyje informacinėmis operacijomis siekiama palaužti visus priešininko galios elementus (politinį, ekonominį, karinį, informacinį)“[43]. Todėl NATO informacinių operacijų sampratoje viešoji informacija bei karinių ir civilinių informacinių veiksmų derinimas užima daug svarbesnę vietą nei JAV doktrinoje.

Kaip ir JAV, NATO apibrėžime akcentuojama informacija ir informaciniai procesai, tačiau papildomai išskiriamas vadovavimas ir kontrolė. Karo su vadovybe ir kontrole samprata yra sena kaip ir patys kariniai konfliktai. Priešo kariuomenės vadovybės eliminavimas visada buvo laikomas vienu iš pagrindinių būdų pasiekti pergalę. Kariuomenė, netekusi savo vadovybės, būtų ne tik demoralizuota – svarbiausia, ji nesugebėtų efektyviai organizuoti ir koordinuoti savo veiksmų. Tačiau informacijos amžiuje nebūtinas fizinis sunaikinimas – užtenka atriboti priešininko vadovybę nuo reikiamos informacijos arba ją iškraipyti, taip atimant iš jos kontrolės galimybę.

NATO taktinėje publikacijoje ATP–3.2 pateikiamas šios organizacijos požiūris tik į puolamąsias informacines operacijas, nors jų apibrėžime akcentuojama ir gynybos nuo šių operacijų reikšmė. Puolamosios informacinės operacijos yra suskirstomos taip: fizinės atakos prieš vadovybę, kontrolę ir komunikacijas, elektroninis karas, operatyvinis saugumas, karinis nuslėpimas ir psichologinės operacijos. Šios priemonės yra analogiškos išdėstytoms JAV doktrinoje, tačiau neįtraukiama specialių informacinių operacijų, už kurias JAV atsako Nacionalinio saugumo agentūra. Tačiau, kaip jau minėta, NATO strategijoje daug didesnis dėmesys nei JAV doktrinoje skiriamas viešosios informacijos ir civilinio bei karinio bendradarbiavimo priemonėms. Viešosios informacijos funkcija – užsitikrinti paramą savo veiksmams konflikto metu. Minėtoje taktinėje publikacijoje viešoji informacija yra skirstoma į karinį ir politinį segmentus. Už karinį viešosios informacijos segmentą atsako

[42] Gardeta J., „Information Operations, the Nato Perspective“ in Bosch J. M. J., Luiijf H. A. M., Mollema A. R., eds. , *Information Operations, NLARMS*, 1999, p. 105.
[43] *Ten pat,* p. 106.

NATO vadovybė, kuri siekia „visiškai ir objektyviai, kiek leidžia operatyvinis saugumas, pristatyti ir paaiškinti visuomenei aljanso pasiekimus“[44] ir garantuoti vidaus ir tarptautinę paramą savo veiksmams. Politinis viešosios informacijos segmentas turi būti užtikrinamas koordinuotais visų aljanso narių veiksmais. Jis labiau nukreiptas į tarptautinės paramos užtikrinimą. Tačiau būtent šiuos veiksmus yra sunkiausia efektyviai įgyvendinti dėl didelio valstybių skaičiaus ir dėl to, kad atsakomybė už juos tenka įvairioms institucijoms ir organizacijoms (karinėms, politinėms, nevyriausybinėms ir pan.).

NATO informacinių operacijų organizavimas ir planavimas taip pat yra panašus į JAV. Čia egzistuoja informacinių operacijų ląstelės analogas – NATO Informacinių operacijų darbo grupė[45], kuriai vadovauja Tarptautinio karinio personalo Operatyvinio padalinio direktorius. Į šią darbo grupę įeina karo su vadovybe ir kontrole, psichologinių operacijų ir kiti specialistai.

Nors konflikto metu NATO ypač akcentuojami strateginio lygio veiksmai, operatyvinis ir taktinis lygiai taip pat yra reikšmingi. Jose Gardeta teigia, kad „operatyviniame lygyje informacinės operacijos papildo pagrindines karinės kampanijos priemones ir yra nukreiptos į priešininko vadovybę ir kontrolę, komunikacijas ir logistiką, o taktiniame lygyje padeda siekti specifinių taktinių uždavinių“[46].

NATO taktinėje publikacijoje, kaip ir JAV doktrinoje, yra išdėstyti principai, kuriais remiantis turi būti vykdomos informacinės operacijos[47]: pirma, karo vado, kuriam tenka visa atsakomybė už informacines operacijas, vadovavimas; antra, visų veiksmų koordinavimas ir integravimas į bendras karines priemones; trečia, tiksli žvalgybinė informacija, kuri turi būti informacinių operacijų pagrindu; ketvirta, visi veiksmai turi būti nukreipti į vadinamąjį priešininko gravitacijos centrą, t. y. į jo pažeidžiamiausias vietas; penkta, informacinės operacijos turi remtis centralizuoto planavimo ir decentralizuoto įgyvendinimo principu; šešta, turi būti aiškiai nustatytas potencialių taikinių sąrašas; septinta, informacinėms operacijoms turi būti ruošiamasi dar prieš prasidedant pačiam kariniam konfliktui, tai ypač taikytina informacinių atakų gynybai; aštunta, vykdant šias priemones turi dominuoti lankstumas ir galimybė prisitaikyti prie vykstančių pokyčių; devinta, turi būti nuolatos įvertinamas panaudotų priemonių efektyvumas.

Jose Gardeta apibendrina NATO požiūrį į informacines operacijas ir teigia, kad „jomis galima paveikti valstybės šerdį, jos infrastruktūrą, pagrindines egzistavimo funkcijas“[48], todėl informacinės operacijos atlieka savotišką atgrasymo funkciją ir „turėtų būti naudojamos taikos metu siekiant krizių prevencijos“[49]. Tačiau tai yra labai sudėtingas uždavinys dėl pačios NATO prigimties. Ši organizacija – tai valstybių sąjunga, kuri dažnai neranda bendros kalbos dėl kur kas paprastesnių klausimų, nei informacinės operacijos. NATO neturi tokios vieningos valios naudoti puolamą-

---

[44] ATP–3.2 Allied Tactical Publication „Information operations, Psichological Operations and Public Information“ p. 3–3.
[45] Gardeta J., (note 40) p. 113.
[46] *Ten pat,* p. 108.
[47] ATP–3.2 Allied Tactical Publication „Information operations, Psichological Operations and Public Information“ p. 3–2.
[48] Gardeta J., (note 40) p. 105.
[49] *Ten pat,* p. 105.

sias ar gynybines informacines operacijas, kokią turi JAV. Visų pirma taip yra dėl to, kad informacinės operacijos yra gana nauja koncepcija NATO karinėje strategijoje. Be to, ji yra sukurta pagal JAV Vieningos Informacinių operacijų doktriną ir neaišku, ar visiškai atitinka šios gynybinės sąjungos poreikius. Antra, (ir, matyt, svarbiausia), šią sąjungą sudaro daugelis valstybių, kurių požiūris į atskirų informacinių priemonių naudojimo galimybes skiriasi. Valstybėse įvairiai suvokiamos teisinės pasekmės, todėl skiriasi apribojimai psichologinėms operacijoms, elektroniniam karui, kompiuteriniams įsilaužimams ir pan. Be to, informacinių operacijų sėkmė didžia dalimi priklauso nuo žvalgybinės informacijos, o NATO šios informacijos turi tik tiek, kiek jos suteikia kiekviena iš valstybių.

6. Karinis konfliktas informaciniame amžiuje: ko Lietuvai derėtų pasimokyti?

Lietuva neturi galimybių savarankiškai vystyti tokių informacinių operacijų programų bei strategijų, kokios yra JAV ir NATO, tačiau tai nėra būtina, nes, mūsų šaliai įstojus į Šiaurės Atlanto aljansą, reikės perimti ir šios gynybinės organizacijos karinius standartus, prisitaikyti prie čia egzistuojančių strategijų ir programų, įskaitant ir informacines operacijas. Šiuo metu esminiai yra du faktoriai. Pirma, derėtų atsižvelgti į tai, kad NATO pagrindinį dėmesį skiria strateginėms informacinėms operacijoms, kur svarbiausią vaidmenį vaidina viešoji informacija. Antra, tarp Lietuvos karo, politikos mokslų ekspertų reikia skatinti diskusiją apie besikeičiantį karinio konflikto pobūdį, nes globali informacinė erdvė neturi ribų, todėl joje vykstantys konfliktai yra potencialiai grėsmingi ir Lietuvai. Derėtų kelti klausimą, kaip tokioje besikeičiančioje saugumo aplinkoje galima efektyviau užtikrinti valstybės piliečių ir tarptautinį saugumą. Todėl ypač svarbu pasirūpinti mūsų valstybės informaciniu saugumu.

6.1. Suderinta viešosios informacijos strategija – raktas į sėkmę

NATO informacinių operacijų programoje viešoji informacija yra laikoma viena iš esminių komponentų įvairiose konflikto arba krizės stadijose: jos pagalba galima išvengti krizės, atgrasyti priešininką nuo tam tikrų veiksmų, o konfliktui prasidėjus – vidaus ir tarptautinei viešajai nuomonei įrodyti savo veiksmų pagrįstumą. NATO taktinėje publikacijoje viešoji informacija yra taip apibrėžiama: „Tai informacija, kuri paskleidžiama arba publikuojama, siekiant kokybiško visuomenės informavimo ir užsitikrinant supratimą bei palaikymą“[50]. JAV informacinių operacijų doktrinoje, kaip ir NATO programoje, viešoji informacija yra skirstoma į informaci-

[50] ATP–3.2 Allied Tactical Publication „Information operations, Psichological Operations and Public Information“, p. 3–25.

ją, skirtą išorės ir vidaus auditorijoms, tačiau NATO dokumente kaip atskira auditorija yra išskiriamos kareivių giminės ir artimieji bei teigiama, kad „prioritetas visada bus atiduodamas šiai auditorijai“[51]. Tai labai svarbus aspektas, turint omenyje Rusijos pirmąją karinę kampaniją Čečėnijoje, kai vietinė žiniasklaida ypatingą dėmesį skyrė rusų karių aukoms ir aukų artimiesiems.

Išorinė viešoji informacija yra nukreipta į žiniasklaidą ir, anot NATO dokumento, turėtų remtis šiais principais: pasitikėjimas yra pagrindas – niekada negalima meluoti žiniasklaidai; kiekvienas karinės operacijos aspektas gali turėti viešumo pasekmes; informacijos ribojimas darosi praktiškai neįmanomas, todėl turėtų būti taikomas tik saugumo sumetimais; negalima teikti prioritetų vienai žiniasklaidos priemonei kitų sąskaita – informacija turi būti prieinama visiems vienodomis sąlygomis; visada reikia stengtis suteikti informaciją; ne visos naujienos yra palankios, bet net ir blogos naujienos turi savo teigiamą pusę (kareivių herojiškumas, pagalbos sužeistiesiems suteikimas ir pan.); žiniasklaida yra pagrindinis informacijos skleidėjas, todėl ji yra reikšminga informacinių operacijų dalis; viešosios informacijos kampanija turi būti vykdoma per visas konflikto fazes; žiniasklaidos susidomėjimas nėra nuolatinis – kartais jį reikia skatinti; NATO pajėgos negali būti atribotos nuo viešosios informacijos; žurnalistai turi būti akredituoti prie NATO[52]. Atkreiptinas dėmesys į tai, kad viešoji informacija apima visą konflikto spektrą: nuo paprastos konkurencijos iki karinės konfrontacijos. NATO programoje numatyta, kad konflikto metu už viešąją informaciją atsako Viešosios informacijos karininkas, kuris naudojasi nuolatiniu ir nenutrūkstamu ryšiu su karine vadovybe.

Šiame dokumente, aptariant viešąją informaciją, dar kartą akcentuojama globalios informacinės erdvės reikšmė ir daroma esminė išvada, kad informacijos kontrolė ir cenzūra moderniame pasaulyje tapo praktiškai neįmanoma ir gali tik pakenkti politiniams ir kariniams tikslams. Tai įvyko dėl technologinių pokyčių, kurių pasekmė – tai karinių ir privačių komunikacijos priemonių atskyrimas ir nepriklausomybė. Ankstesniuose kariniuose konfliktuose, pavyzdžiui, Vietname, žiniasklaidai taip pat buvo teikiamas svarbus vaidmuo, tačiau drauge buvo bandoma kontroliuoti žurnalistų perteikiamą informaciją, nes žurnalistų veikla priklausė nuo to, ar kariuomenė suteikia komunikacijos priemonių reportažams perteikti, ar ne. Atsiradus nešiojamiems kompiuteriams, videotelefonams ir kitoms priemonėms, žurnalistai tapo nepriklausomi nuo kariuomenės technikos. Todėl norėdama efektyviai vykdyti viešosios informacijos kampaniją, NATO turėjo prieiti prie tam tikrų išvadų: pirma, esminis bendravimo su žiniasklaida metodas tapo „atvirumas žiniasklaidai ir nepriklausomai žurnalistikai“[53], antra,– tai nebestebina po karinio konflikto Irake patirties, – žurnalistų įtraukimas į karinius padalinius siekiant tam tikro emocinio prieraišumo prie karių ir paramos jų vykdomoms užduotims; žiniasklaidos pranešimai negali būti cenzūruojami nepriklausomai nuo to, ar jie perteikiami per privačius, ar per NATO komunikacinius kanalus; informacijos saugumas turi būti užtikrinamas šaltinio, o ne informacijos perteikėjo – žurnalisto lygmenyje. Taigi iš viešosios informacijos strategijos dingo tokie anksčiau svarbūs žodžiai, kaip informacijos kontrolė ir cenzūra.

---

[51] *Ten pat,* p. 3–30.
[52] *Ten pat,* p. 3–30.
[53] *Ten pat,* p. 3–30.

Vidaus komunikacija kiekvienoje organizacijoje yra labai svarbi funkcija. Kariuomenėje ji palaiko karių moralę ir ryžtą. NATO vidaus viešosios informacijos priemonės yra vidiniai laikraščiai, žurnalai, biuleteniai, radijas, televizija bei kt. priemonės. Be to, kariams bendrauti su artimaisiais garantuojama saugi ir greita pašto tarnyba, elektroninio pašto priemonės.

Kitas svarbus viešosios informacijos aspektas – tai mokymai ir pratybos visiems NATO kariuomenės atstovams – tiek paprastiems kariams, tiek karininkams. Taktinė publikacija numato, kad NATO personalas turi dalyvauti kursuose „Žiniasklaida šiandien“, „Žiniasklaida ir žmogaus teisės“, „Kaip atsakyti į žurnalistų klausimus“, „Saugumas šaltinio lygmenyje“ , o personalo vadovai ir karininkai – kursuose „Susitikimo su žurnalistais planavimas“, „Kaip perteikti žinią“, „Interviu principai“, „Brifingai“[54] .

6.2. Informacinis saugumas ir Lietuvos pasirengimas

Nepriklausomai nuo Lietuvos narystės NATO, mūsų šaliai būtina užsitikrinti nacionalinės informacinės infrastruktūros saugumą. Pavyzdžiu galėtų būti ir mūsų Rytų kaimynas: 2000 m. rugsėjo 9 d. buvo patvirtinta Rusijos Federacijos informacinio saugumo doktrina, kuri „yra Nacionalinio saugumo koncepcijos tęsinys informacinėje srityje […], formuoja valstybės politiką informacinio saugumo srityje, […] rekomenduoja, kaip tobulinti teisinę bazę, […] skatina kurti tikslines informacinio saugumo programas“[55] .

Tačiau Lietuvai tikslingiausia būtų remtis nedidelės Europos valstybės Austrijos požiūriu į informacinį saugumą. A. A. J. Forstner – Billau, aprašydamas šios valstybės patirtį, teigia, kad nacionalinę informacinę infrastruktūrą sudaro trys tarpusavyje susiję sluoksniai: privati, federacinė (arba vyriausybinė) ir karinė informacinės infrastruktūros. Siekiant efektyvaus saugumo, būtina apsaugoti visas šias infrastruktūras. Karinė infrastruktūra visada būna geriausiai apsaugota, nes remiasi vienodų standartų ir reikalavimų diegimu bei mokymu. Daugelis valstybių panašią politiką bando pritaikyti ir vyriausybinėms informacinėms infrastruktūroms, tuo tarpu daugiausiai problemų kyla dėl privačios infrastruktūros nesaugumo. „Nacionalinė informacinė infrastruktūra, kuri yra modernios visuomenės stuburas, yra neleistinai pažeidžiama nusikaltėlių, teroristų ar priešiškai prieš valstybes nusiteikusių asmenų veiksmų“[56] . JAV informacinių operacijų doktrina atskleidė tai, kad didžiosios valstybės investuoja didžiulius finansinius resursus į šią sritį. Tuo tarpu mažąsias valstybes galima būtų suskirstyti į tris grupes: Austrijos tipo valstybės, kurios suvokia šią problemą ir bando ją spręsti, kita grupė net nesuvokia šios problemos, o Lietuva ir kitos panašios valstybės šios problemos neakcentuoja, tačiau, kaip paradoksalu bebūtų, kopijuodamos užsienio valstybių patirtį iš dalies ją sprendžia.

---

[54] *Ten pat,* p. 3–31.

[55] Доктрина информационной безопасности Российской Федерации, http://www.scrf.gov.ru/Documents/Decree/2000/09-09.html 06 09 2003.

[56] Forstner–Billau A. A. J., „Information Operations: Ideas for a Strategic Approach in a Small Country“ in Bosch J. M. J., Luiijf H. A. M., Mollema A. R., eds., *Information Operations, NLARMS*, 1999, p. 231.

Informacinio saugumo klausimais Lietuvoje susirūpinta, kai, ruošiantis narystei ES, buvo siekiama perimti „Europa“ programos priemones: „Informacinių technologijų dėka didinti sudaromų sandorių saugumą, pradedant technologiniais sprendimais ir baigiant teisinėmis priemonėmis“[57]. Be to, 2001 metų lapkričio 23 d. Europos Tarybos iniciatyva Vengrijos parlamente 30 Europos valstybių pasirašė konvenciją dėl kovos su didėjančia elektroninių nusikaltimų grėsme. „Remiantis sutartimi, pasirašiusios valstybės įsipareigojo steigti nacionalinius nuolat veikiančius centrus, teikiančius savitarpio pagalbą visais su kompiuteriniais nusikaltimais susijusiais klausimais, pradedant kompiuteriniais įsilaužimais ir išeikvojimais ir baigiant grėsmę gyvybei keliančiais sunkiais nusikaltimais“[58]. Tačiau Lietuvoje dėmesys skiriamas tik valstybinei informacinei infrastruktūrai.

JAV informacinių operacijų doktrina karinę informacinę infrastruktūrą laiko geriausiai apsaugota, tačiau dėl to, kad ji yra praktiškai neatsiejama nuo vyriausybinės ir privačios informacinių infrastruktūrų, ji taip pat pažeidžiama. Geriausiai problemą dėl privačios infrastruktūros pažeidžiamumo apibendrina A. A. J. Forstner – Billau: „Seniau informacinės technologijos versle buvo diegiamos kaip vienetinės sistemos, kurios praktiškai neturėjo jokių sąryšių su kitomis sistemomis, todėl skyrėsi ne tik pačios technologijos, bet jos buvo ir nesuderinamos – dabar nuosekliai ir nepaliaujamai bandoma spręsti šią problemą“[59], o informacinių technologijų korporacijos uždirba nemažai pinigų. Dabar besivystantis Rytų Europos valstybių verslas diegia gerokai pažangesnes technologijas, kurios privalo atitikti bendrus, įskaitant ir saugumo, standartus, nes to reikalauja verslo logika. Tačiau A. A. J. Forstner – Billau mano, kad privačios informacinės infrastruktūros apsaugos procesą galima paspartinti: „reikia į rinką pritraukti geros kokybės informacinės apsaugos produktus, kurie yra brangūs ir dažnai neįperkami vietiniam verslui, todėl mažos valstybės verslas turėtų būti patrauklus didžiųjų korporacijų investicijoms, dalis iš kurių būtų skiriama informacijos apsaugai“[60].

Mažų valstybių vyriausybinės informacinės infrastruktūros susiduria su analogiškomis problemomis, kaip ir privatus sektorius. Viešojo administravimo informacinės sistemos kūrėsi taip pat nekontroliuojamos – tai buvo atskirų ministerijų ar agentūrų informacinės sistemos, nederinamos tarpusavyje. Tačiau informacinio saugumo problemos sprendimas viešojo administravimo sektoriuje turi esminį privalumą – čia egzistuoja galimybė patikėti problemos sprendimą konkrečiai institucijai ir pareigūnams, kurie už tai atsakytų. Austrijoje Federacinėje kanceliarijoje buvo įsteigta taryba Informacinių technologijų suderinamumo klausimams spręsti[61].

2001 metais Lietuvos Respublikos Vyriausybė, kurdama palankias sąlygas saugiai informacinės visuomenės ir elektroninės valdžios plėtrai, informacinių technologijų saugos veiksmų koordinavimą valstybiniame sektoriuje pavedė vykdyti Vidaus reikalų ministerijai. Ministerija parengė Informacinių technologijų saugos valstybinę strategiją bei jos įgyvendinimo priemonių planą, siekiantį 2005 metus. Abu šie

---

[57] IT sauga: valstybės institucijų sauga, Informacinės visuomenės plėtros komitetas, http://www.ivpk.lt/main-aktual.php?cat=61&n=8 06 09 2003.
[58] *Ten pat.*
[59] Forstner–Billau A. A. J., (note 54) p. 231.
[60] *Ten pat,* p. 233.
[61] *Ten pat,* p. 234.

dokumentai nustato saugumo užtikrinimo principus, būtinas įgyvendinti priemones, kurios apima teisinės bazės plėtrą, rekomendacijų ir metodikos rengimą, specialistų mokymus, svarbiausių valstybės informacinių sistemų saugos stiprinimą bei visuomenės švietimą[62]. Vidaus reikalų ministerijos Informacinės politikos departamento direktoriaus Aurimo Matulio teigimu, „strategija pabrėžia, kad saugumas turėtų būti garantuojamas kompleksiškai, diegiant programines, technines, fizinės saugos ir, žinoma, administracines priemones“[63]. Reiktų atkreipti dėmesį, kad strategija pabrėžia informacijos reikšmingumo principą, kuris yra vienas esminių tiek JAV, tiek NATO informacinio saugumo sampratose. Anot A. Matulio, „saugos priemonės turėtų atitikti resursų, kuriuos siekiama apsaugoti, vertę ir galimus jų pažeidimo padarinius – ne kiekvienai sistemai reikia maksimalios saugos, todėl diegtinos saugos priemonės pasirenkamos atsižvelgiant į jų reikšmę ir būsimas saugos sąnaudas“[64]. Be šio, strategija numato ir kitus principus: aplinkos stebėjimo, informacijos technologijų saugos sistemos ir informacinių sistemų tarpusavio priklausomybė, informacijos technologijų naudotojų ir specialistų švietimas[65]. Pastarasis principas yra pabrėžiamas ir JAV informacinių operacijų doktrinoje. Jis ypač svarbus, nes, anot A. Matulio, „informacinių technologijų saugumas organizacijose didžia dalimi – apie 70 % – priklauso nuo žmogiškojo faktoriaus bei organizacinių procesų ir tik apie 30 procentų – nuo technologinių priemonių“[66].

Minėtai strategijai 2002–2004 m. įgyvendinti numatyti 3,2 mln. Lt. Be to, siekiant įdiegti saugumo valdymo principus valstybės institucijose Vyriausybė patvirtino Bendruosius duomenų saugos reikalavimus[67]. Jie nustato, kad valstybės institucijos turės parengti ir, suderinusios su Vidaus reikalų ministerija, patvirtinti saugumo politiką bei užtikrinti jos laikymąsi savo veikloje. Reikalavimai buvo suderinti ir su Lietuvos savivaldybių asociacija, todėl jais rekomenduojama vadovautis ir savivaldybėms[68].

Svarbus ir A. Matulio teiginys, kad „Lietuvai sėkmingai integruojantis į NATO bei Europos Sąjungą būtina tinkamai pasirengti kartu saugiai dirbti elektroninėje erdvėje, užtikrinti saugų pasikeitimą informacija tarp mūsų šalies ir tarptautinių organizacijų bei užsienio šalių“[69]. Todėl Valstybės saugumo departamentas, Krašto apsaugos ir Vidaus reikalų ministerijos kartu kuria saugumo sistemą, garantuosiančią saugų elektroninių valstybės paslapčių apdorojimą, saugojimą bei perdavimą kompiuterių tinklais. Šioje srityje atliekamus Lietuvos specialistų darbus gerai įvertino NATO bei JAV ekspertai[70].

---

[62] *Lietuvos Respublikos Vyriausybės nutarimas Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo,* 2001 m. gruodžio 22 d. Nr. 1625.

[63] Siekiama užtikrinti informacinių technologijų saugumą Lietuvoje, Vidaus reikalų ministerija http://www.vrm.lt/nuorodos/rvs/sp030108.htm 06 09 2003.

[64] *Ten pat.*

[65] *Lietuvos Respublikos Vyriausybės nutarimas Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo,* 2001 m. gruodžio 22 d. Nr. 1625.

[66] Siekiama užtikrinti informacinių technologijų saugumą Lietuvoje , Vidaus reikalų ministerija http://www.vrm.lt/nuorodos/rvs/sp030108.htm 06 09 2003.

[67] *Lietuvos Respublikos Vyriausybės nutarimas Nr. 2105 Dėl duomenų saugos valstybės ir savivaldybių informacinėse sistemose,* 2002 m. gruodžio 31 d.

[68] Siekiama užtikrinti informacinių technologijų saugumą Lietuvoje , Vidaus reikalų ministerija http://www.vrm.lt/nuorodos/rvs/sp030108.htm 06 09 2003.

[69] *Ten pat.*

[70] *Ten pat.*

Išvados

Informacijos amžiuje vyks postmodernūs kariniai konfliktai, kai globalioje informacinėje erdvėje valstybės ir kiti tarptautinių santykių subjektai sieks įtvirtinti savo politiką jėgos priemonėmis. Tačiau šie konfliktai nebebus panašūs į Clausewitz modelį, kai vadovai iškelia politinius tikslus ir kontroliuoja karius, kariai tiesiogiai kariauja ir yra teisėti smurto taikiniai, o civiliai nedalyvauja konflikte, bet remia savo vadovus mokesčiais bei palaiko jų iškeltus politinius tikslus. Informacijos amžiaus konfliktas – tai ikivestfalinis konfliktas, kai nusikaltimai prieš civilius ir valstybės vidaus tvarką buvo norma. Tačiau konflikte naudojamos priemonės bus pačios moderniausios.

Valstybės turi ieškoti naujų būdų savo piliečių saugumui užtikrinti. JAV bei kitos didžiosios valstybės mano, kad sėkmę ateities konfliktuose gali užtikrinti informacinis dominavimas globalioje informacinėje erdvėje, o tai galima pasiekti informacinių operacijų pagalba. Ypatingą reikšmę šių operacijų metu turi viešosios informacijos priemonės bei karinės ir civilinės sferų informacinių veiksmų derinimas. Tokią strategiją yra paruošusi NATO, todėl Lietuvai reiktų perimti šią patirtį.

Informacijos amžiuje valstybės savo gerovę sieja su informacinės visuomenės, žinių visuomenės, elektroninės vyriausybės ir pan. programomis. Tačiau informacija gali būti ne tik gamybos, bet ir griovimo pagrindas, todėl kiekviena valstybė ypatingą dėmesį turi skirti informaciniam saugumui. Lietuva jau žengė pirmuosius žingsnius šioje srityje: parengtos Informacinių technologijų saugos valstybinė strategija bei jos įgyvendinimo priemonių planas iki 2005 metų. Tačiau dar daug ko galima būtų pasimokyti iš Austrijos patirties.