УДК: 659.23 : 004.056.5 : 343.534

ЕКОНОМСКА ШПИЈУНАЖА И НОВЕ ТЕХНОЛОГИЈЕ У ГЛОБАЛИЗОВАНОЈ МЕЂУНАРОДНОЈ ЗАЈЕДНИЦИ

Слободан Нешковић
Универзитет Привредна академија у Новом Саду,
Факултет за економију и инжењерски менаџмент

Економска шпијунажа у савременој међународној констелацији обухвата велики број специфичних мера и поступака агресивног карактера чији је циљ угрожавање супарника на светском тржишту. Применом легалних и нелегалних средстава, веома често неспојивих са етичким постулатима пословања, тежи се елиминисању конкурената. За разлику од обавештајне делатности, међународна економска шпијунажа користи све расположиве методе, од медија до најсуровијих поступака, чак и у надметању традиционалних савезника. Глобална супрематија САД, праћена тријумфалистичком прекоокеанском политиком националне безбедности, утицала је на коренито редизајнирање структуре међународне заједнице. Информатичко- комуникациони ресурси и феномен знања одређују позицију појединих земаља у планетарној заједници. Технолошки доминантни субјекти у процесима глобализације формирају нови комуниколошки поредак са злоупотребом медија, јавног мњења и осталих чинилаца друштва. Значајну улогу имају информационе инфраструктуре које се инаугуришу у све сфере јавног живота, а у контексту реализације националних интереса, што производи постмодерне изазове и ризике у међународним односима. То посебно погађа мале и неразвијене земље, угрожавајући њихов опстанак и темеље међународног система.

Кључне речи: *економска шпијунажа, нове технологије, информациона инфраструктура, глобализација, САД, безбедност, међународна заједница*

Увод

Савремени систем међународних економских односа обновљен је после завршетка Другог светског рата, када су на конференцији у америчком граду Бретон Вудсу усвојени основни принципи о формирању међународног финансијског и монетарног система. Неколико година касније формиран је ГАТТ, у чијем статуту су кодификовани адекватни принципи међународног система трговине, што је 1995. године формулисано у оснивачким документима Светске трговинске орга-

низације, на који начин је постављен темељ и дефинисан правац обликовања послератног међународног економског поретка.

Модерно доба, каналисано процесима глобализације, карактерише се стицањем надмоћи у планетарним разменама, што представља резултат не само војне, већ и економске, технолошке и развојне супремације над противницима. Као што је некада оружје представљало основни аргумент доминације, данас је то информација, као четврти обавезни чинилац производње, поред капитала, радне снаге и технологије. Информација је најбитнији чинилац остваривања предности над конкуренцијом и због тога најразвијеније земље света све више својих обавештајних ресурса користе ради прибављања брижљиво чуваних индустријских, производних или финансијских информација, које ће држави или домаћој компанији омогућити боље позиционирање на глобалном тржишту.

Економска шпијунажа представља скуп добро планираних и веома стручно изведених активности чији је циљ прибављање поверљивих економских информација, које су од користи за пословне пројекте фирме или заштиту економских интереса властите државе. У суштини, економска или индустријска шпијунажа значи нелегално прикупљање економских (индустријских) података и информација, које конкурентске фирме чувају у тајности. У ту сврху користе се средства као што су запошљавање својих људи у конкурентским компанијама, ангажовање специјализованих агенција, коришћење дипломатских представника у иностраним земљама где компанија има пословне интересе итд.

Послови и делатности из области економске шпијунаже имају превасходни циљ доласка у посед пословне тајне одређеног државног субјекта или компаније. Првобитни облици пословне тајне појављују се још у старом веку у области занатства, а свој пуни смисао овај институт добија у капитализму, развојем конкуренције на тржишту. Пословна тајна може се дефинисати као скуп докумената и података чије саопштавање трећем лицу може нанети штету пословним интересима и пословном угледу компаније. Такође, присутан је и став да је пословна тајна субјективно право којим се искључује право коришћења истих података од стране другог.

Тајна подразумева сваки онај податак о једној држави (предузећу, државном органу, друштвеној организацији – странка, синдикат, удружење бораца итд. – разним установама као што су институти, универзитети, социјалне службе итд.), који је од битне важности за ту институцију и чије би сазнање од стране неовлашћених лица могло да проузрокује конкретне штете, како за ту институцију и установу, тако и за државу у целини. Према томе, за једну земљу нису тајни подаци само војни, политички и економски него и технолошки, социјални, културни, образовни, туристички, спортски и други који би могли послужити другој држави да лакше оствари своје одређене циљеве и нанесе штету држави о којој располаже таквим подацима.

Главни изазов током следеће деценије биће како побољшати приступ, комуникацију и употребу просторних података ради пружања подршке мноштву одлука на свим нивоима друштва. Позивање на географске податке потребно је у областима као што су здравство, образовање и социјална политика, где се мноштво информација које су сакупљане из разних извора користи како би се пратили проблеми и идентификовале тенденције. Можда је тренутно најизраженија потреба за просторним подацима и информацијама у сфери управљања животном средином.

Да би се постигли циљеви као што су одржив економски развој и заштита осетљивих природних богатстава, планери и власници земљишта морају да знају које информације су им на располагању, како да их добију и како се могу повезати са информацијама из других извора. Нове технологије (ГИС, ГПС, даљинско осматрање и просторно моделирање) пружају могућност да се изађе у сусрет овим и другим потребама.

Међународна економска шпијунажа

Међународна економска шпијунажа и обавештајна делатност воде порекло из античких времена, при чему се прве познате активности из ове области везују за Мојсија, што је записано у *Књизи бројева Библије Јерусалимске,* као неуспешно спроведен подухват дванаест Јевреја шпијуна који су упућени да извиде Обећану земљу, државу Канаан. Поред наведеног, познате су шпијунске активности великих историјских личности и освајача као што су Хамураби, Одисеј, Јулије Цезар, Џингис Кан, Луј XI и Наполеон. Значајне студије о шпијунажи представљају учења познатог стратега древне Кине, Сун Цеа, затим Индијца Каутилија, сер Френсиса Валшингама, кардинала Ришељеа и оца Жозефа.

Савремени концепт међународне економске шпијунаже заснива се на делима америчких теоретичара Харолда Виленског и Мајкла Портера, као и на радовима Швеђанина српског порекла Стевана Дедијера. Као претеча систематског проучавања економске шпијунаже у међународним односима, Харолд Виленски у свом делу *Организациона шпијунажа: знање и политика у влади и индустрији,* покреће две основне тематске целине у овој области. Прва је примена колективне стратегије у формулисању заједничког концепта за стварање конкурентске предности на тржишту, док друга потенцира значај сазнања у економији и индустрији као стратегијског покретача развоја. Значајан допринос модерној концепцији економске шпијунаже промовише и Стеван Дедијер. Он истиче важност прикупљања пословних информација и њихов тренд у савременој међународној заједници.[1]

Једна о кључних промена у свету јесте да на глобалном тржишту државе почињу да губе примат, који од њих преузимају тзв. транснационалне компаније, које постају кључни чиниоци интегралног глобалног система. С обзиром на то да ове компаније захтевају велике количине квалитетних информација за своје потребе, оне почињу да развијају сопствене обавештајне капацитете, чиме се ослобађају зависности од државних институција те намене. То доводи и до померања моћи са држава на транснационалне компаније.

На основу наведеног, пословна шпијунажа могла би се дефинисати као збир веома деликатних, планираних и стручно изведених активности на прибављању поверљивих информација од користи за пословне пројекте сопственог предузећа, организације или државе или за заштиту њихових пословних интереса. Да бисмо се ближе упознали са начинима приступа поверљивим информацијама, неопходно

[1] Dedijer, S., *Development and Management by intelligence/Japan*, 1991, pp. 9.

је утврдити које информације су најчешћа мета економских обавештајних операција. Оне су подељене на пет група: [2]

- финансијске,
- организационе,
- маркетиншке,
- техничке,
- научне.

Опште је познато да се преко 95% потребних информација у економској обавештајности може добити и добија легалним путем. Постоји више начина да се до тражених информација дође без коришћења нелегалних средстава или метода: интернет представља најлакши и највише коришћен начин проналажења информација о економским субјектима. Према неким истраживањима, између 1990. и 1995. године дошло је до повећања економске обавештајне активности од преко 300%, и за то је, као главни кривац, означен интернет и информације које он пружа. Најчешћи начин за добијање информација је путем електронске поште, као и путем разних упита. Евидентно је да је информатичка образованост запослених прилично ниска када се ради о безбедности на интернету. Приступ друштвеним мрежама типа Фејсбук, Мајспејс, Твитер или разним чет-собама представља велику опасност за сваку компанију, јер су запослени склони да у необавезним разговорима чак и потпуним странцима причају врло поверљиве ствари. Популарности интернета, као начину за прибављање поверљивих информација, доприноси и анонимност, коју је много лакше остварити путем интернета него у неким другим ситуацијама. Могућност широкопојасног приступа интернету са јавних места, попут библиотека или интернет кафеа, пружа велике могућности за потпуно анониман економско-обавештајни рад. Претрага запослених је уобичајен начин добијања информација.

С обзиром на то да не постоји намера да се интервјуисани запосли, ова метода је врло неетичка, а у неким ситуацијама може се сматрати и шпијунском делатношћу. Заједничка улагања и спајања фирми представљају још један начин легалног долажења до битних информација. Ако запослени из фирме А дуже време раде заједно са запосленима из фирме Б, може се очекивати да ће се временом сматрати за партнере, па попуштају безбедносни протоколи и омогућава им се приступ информацијама и технологијама.

Такође, још једна сигурна солуција за долазак у посед тражене технологије представља куповина или преузимање компаније, али је то прилично скупо решење. Конференције, изложбе, семинари и сајмови представљају добро место да се у директном контакту извуку важне информације. Због знања и стручности учесници су често ангажовани од компанија или влада ради прибављања информација. Директне посете су дуго биле вредан извор информација из технолошких или производних компанија. Посетиоци су обучавани како да дођу до вредних информација намерним уласком у забрањене зоне, недозвољеним фотографисањем или постављањем питања изван дозвољених оквира.

Иако представљају само мали део економских обавештајних података, подаци добијени на нелегалан начин често су највреднији, пошто су толико важни да се до њих не може доћи легалним путевима. Организовани криминал постао је врло чест начин за доби-

[2] Luttwak, E., *From Geopolitics to Geo-economics,* The national interest, 20, 1990, pp. 17.

јање информација из предузећа. Глобализација бизниса омогућила је и неке нове транснационалне облике криминала. Тако се криминалци не либе да притиском и уценама на пословне људе уђу у највеће компаније и својом снагом и моћи, која је често већа од локалних власти, представљају велику опасност за бизнис и индустрију. Независни предузетници укључују независне или слабо повезане особе у економској шпијунажи. У суштини, ради се о приватним детективима које унајмљују компаније ради прибављања информација које компанија унајмљивач сматра потенцијално корисним за себе.

Без обзира на то ко је лице које прибавља информације, постоји неколико начина на које компаније или чак стране владе прибављају информације. Запослени (инсајдери) са правом приступа представљају велики безбедносни проблем за компаније. Према неким истраживањима, преко 75% економске шпијунаже обавља се преко инсајдера, особа које долазе из саме фирме или имају приступ осетљивим подацима. Наравно, постоји одређен број људи који ненамерно одају тајне које не би смели. Такође, користи се изнајмљивање информација од стране обучених професионалаца, који на посредан и вешт начин збуњују жртву и наводе је да ода ствари које иначе не би. То се назива социјални инжењеринг и, иако само по себи није кривично дело, може бити увод у даља кривична дела.

Инфилтрација међу запослене представља добар метод шпијунских активности. Имајући у виду да се без већих тешкоћа у великом броју случајева може ући унутар субјекта шпијунаже помоћу фалсификованих лажних докумената, овим приступом степен успеха шпијунаже је драстично повећан.

Регрутација запослених је један од најефикаснијих начина шпијунаже. Једном када се инсјадер или „кртица“ регрутује помоћу мита или неког другог начина, може му се тражити посебна врста информација, а не све на шта наиђе. Сакупљач информација не треба да буде фокусиран на извршне директоре или истраживаче, већ ће много више постићи регрутацијом нижег особља, као што су секретарице, рачунарски техничари или чак и особље одржавања. Овде постоје две предности: нижи нивои запослених много су мање сумњиви, а често имају већи приступ информацијама и њихова цена може бити много нижа, а воља за сарадњом много већа него рецимо генералног менаџера. Овај начин шпијунаже је прилично лак, јер један број запослених и на своју руку краде информације ради даље продаје, док су други незадовољни односом према њима и као створени за овакву врсту сарадње.

Компјутерски упади представљају још један, веома чест начин за прибављање информација. С обзиром на то да се рачунари све више користе за обраду и складиштење података, све је већи број „упада“ у системе корпорација ради нелегалног прибављања информација. Док један број такозваних хакера то ради из чистог спорта или мржње према глобализацији или мултинационалним компанијама, постоје и професионалци који краду информације ради продаје на црном тржишту. И конкурентске компаније и обавештајне службе унајмљују овакве професионалце ради провaљивања у туђе информационе системе. Рачуна се да је преко 90% компанија било бар једном жртва упада у информациони систем, док су директни губици само у 2002. години износили преко 170.000.000 долара због крађе информација.

Провале и крађе представљају традиционалан начин за прибављање обавештајних података. Иако се у већини случајева ради о физичкој крађи докумената, приликом које се они отуђују, може се десити да провалник само фотографише или умножи

тражени документ, тако да жртва и не зна да је покрадена и нормално наставља рад на пројекту, што конкуренцији омогућава праћење развоја и даље информације. Овај начин обично је повезан са осталим начинима економског обавештавања.

С напретком технике електронски надзор се све више користи, па је, на пример, могуће издвојити један глас између хиљаде гласова на стадиону или прислушкивати мобилни телефон жртве. Док је раније ова опрема била ексклузивитет државних обавештајних служби, данас је могуће за мало новца купити најквалитетнију опрему за прислушкивање и надзор.

Као што се види, широк је дијапазон средстава и техника за долажење до информација. Традиционалне тржишне утакмице претварају се у праве ратове, и ту циљ оправдава свако средство, те свака компанија мора да мисли првенствено на сопствену безбедност.

Школе економске шпијунаже

Претходни део текста посвећен је разматрању есенцијалних постулата економске шпијунаже и начинима прикупљања информација. Међутим, све велике економије развиле су своје посебне системе економске шпијунаже или чак и посебне школе за обуку економских обавештајаца, такозване „школе за економско ратовање". У даљем сагледавању феномена обавештајности и шпијунаже, анализираћемо појединачне приступе, концепте у овом сегменту, на примеру најутицајнијих држава у свету.

Сједињене Америчке Државе

Као једина стварна суперсила, у војном и економском смислу, Сједињене Државе су нарочито у другој половини 20. века предњачиле у домену економске шпијунаже. Полазећи од чињенице да су америчке фирме водеће у технолошким проналасцима, увек је присутна реална опасност од шпијунаже, која се свакодневно дешава. Посебну потешкоћу представља америчка транспарентност, која омогућава страним обавештајним елементима да скоро 90% тражених информација добију из легалних извора, без коришћења нелегалних начина. Мета су како цивилне, тако и војне технологије, а шпијунирају сви, без разлике, како непријатељи тако и савезници. Присутност шпијунаже америчких компанија је толика да се рачуна да САД годишње губе између 100 и 250 милијарди долара[3] због конкурентских шпијунских активности.

За време такозваног „хладног рата" против СССР-а америчка обавештајна делатност била је усмерена претежно на војне капацитете и технологије, да би се у времену после тога полако пребацивала у сферу економске шпијунаже. Приличан заокрет у томе представља победа Била Клинтона на председничким изборима 1992. Он формира Национални економски савет, чија је претежна улога побољшање компетитивности у америчкој трговини и привреди.[4] Пажња се усмерава на развијајућа нова тржишта, а

[3] Петровић, З. П., *Економска шпијунажа*: *мали водич кроз историју економске обавештајности, до десете револуције човечанства*, Београд: Драслар партнер – Центар Југоисток, 2005, стр. 94.

[4] Исто, стр. 94.

прикупљање економских података постаје један од најважнијих задатака обавештајних служби. Охрабрују се компаније да добијене обавештајне податке деле између себе ради свеукупног побољшања компетитивности, док ЦИА издаје дневни брифинг економске шпијунаже, у којем су садржани подаци добијени економском шпијунажом.

Поред наведеног, америчка влада спроводи и агресивно лобирање код страних држава у корист америчких компанија, ради добијања уносних послова. Као крајње средство користи се војна моћ, тамо где друга средства закажу. Проблем који постоји у америчкој привреди јесте култура, која форсира индивидуализам, тако да се често разилазе лични и државни циљеви, што отежава постизање јединствених циљева. У посао економске шпијунаже укључене су све обавештајне структуре: ЦИА, НСА, војне агенције, шпијунски сателити војске, односно системи за прислушкивање, као што су „Ешелон", „Велике уши" и друге. Преко ових високотехнолошких и софистицираних пројеката, влада САД сваког дана прикупља и анализира огроман број података, из којих се издвајају битне и као такве у фази распарчавања информација достављају одговарајућим друштвеним субјектима.

Јапан

Јапан поседује специфичну технолошку инфраструктуру у сфери економске шпијунаже. Земља која је из Другог светског рата изашла разорена, са огромним губицима и две атомске бомбе бачене на њену територију, брзо се опоравила и заузела значајно место на светској економској позорници. Главне разлоге томе треба тражити у неколико специфичности. Пре свега, Јапан се веома разликује од осталих западних савезника: према удаљености од осталих држава, посебности језика и културе. Ову државу одликује висок степен патриотизма, док је јапанска елита на време схватила да је једини пут опоравка Јапана економски опоравак земље. Јапански менаџмент има јединствен приступ управљању предузећима, где се сваки запослени осећа као део породице и апсолутно је лојалан једној заједничкој идеји – освајању светског тржишта. У Јапану су испреплетани многобројни чиниоци економског развоја земље: МИТИ (Министарство за међународну трговину и индустрију), ЈЕТРО (Јапанска спољно-трговинска организација), као и највеће компаније, синдикалне организације и обавештајне службе.

Најбитније карактеристике пројекта јапанске економске шпијунаже јесу:

• интензивно коришћење информација у офанзивној политици индустријског развоја, као и приступ конкурентским сазнањима;

• динамично управљање тајнама, уз јасно означавање стратегијских тајни које се по сваку цену штите од осталих држава.

Основу чини делљивост информација, која је свеприсутна, јер доприноси заједничким циљевима. Такође, велика пажња поклања се утицајности у свету, лобирању, а за економско обавештајца користи се сваки Јапанац у било којој земљи у свету који може да буде од користи.

Јапанска Мацушита школа за бизнис и менаџмент, у којој се школује пословна елита Јапана, и која представља најбољу установу те врсте, гарантује Јапану дугорочну предност на пољу економске обавештајности, јер квалитетан кадар, уз културу јединства и заједничког циља, сигуран је гарант за то.

Француска

Француска је прва у свету основала школу за обучавање економских обавештајаца, под називом Школа за економско ратовање. Французи имају неколико стотина агената ангажованих у индустријској шпијунажи у корист државе, које зову „генерали спољне безбедности". Они су једина држава која у економском обавештајном рату нема проблема да се замери чак и САД, од којих сви зазиру. Основа француске економске шпијунаже је економска одбрана земље. Компанијама се даје велика аутономија, а истовремено се стимулишу да размењују искуства и податке ради заједничког напретка, као и стварање заједничких информационих мрежа. Представљају главног обавештајног противника за САД у Европи. Главна служба је ДГСЕ (Генерална дирекција спољне безбедности).

Израел

Главна институција економске шпијунаже у Израелу је ЛАКАМ (Канцеларија за специјалне задатке), што је пандан за шпијунске задатке. Иако савезници САД, Израелци се не либе шпијунских операција против њих. Највећи успех представља крађа обогаћеног уранијума од САД, што им је омогућило да развију сопствено нуклеарно наоружање, које је главни гарант опстанка њихове државе међу непријатељским арапским државама. Посебна област ангажовања у сфери међународне економске шпијунаже обухвата крађу нове војне технологије.

Кина

Кина представља нарастајућу економску и обавештајну силу. Преко 70.000 људи укључено је у обавештајни рад под окриљем ИСТИЦ (Институт за научну и технолошку информацију Кине). Последњих десет година шпијунирају посебно САД, и то у сфери високих технологија попут рачунарских и космичких. Посебан случај је убацивање агента у Лос Аламос, америчку лабораторију за развој нуклеарног оружја, што се до тада сматрало немогућим. Велики проблем представља кинеска пиратерија познатих робних марки, чиме се крши право интелектуалне својине. Да би натерали Кинезе да поштују међународне законе, примили су Кину у СТО (Светску трговинску организацију), али то није решило проблем, који је свеприсутан захваљујући првенствено одличној обавештајној служби, која је способна да прибави информације о сваком производу који занима кинеску привреду.

Савремене технологије и друштвена моћ

Промене политичких односа на глобалној светској сцени резултат су америчке доктрине ниског интензитета и тоталитарне идеологије новог поретка, ради стварања бројних патуљастих држава које ће постати потенцијално тржиште за мултинационалне корпорације и јефтини извори радне снаге и природних сировина.

За разлику од свих претходних ратова, када је приоритет даван масовности, наоружању и национално-патриотским осећањима, данас се борба одвија у свести човека посредством масмедија и сличних информатичко-интелигентних оружја. Редефинисање метода, техника и инструментарија специјалног рада подразумевало је изградњу софистицираног, суперкорективног протока информација, са задатком униформисања јавног мњења, као психолошке подлоге за наставак интервенције војним средствима или политички притисак за промену владајућег курса. При томе, извори доминације крију се у технолошкој супериорности која водећим државама омогућава неприкосновен положај у домену располагања инфорамцијама.

Водити ратове могу само они који господаре информацијама, јер они који их поседују владају планетом. Према резултатима истраживања обављеног за потребе Европског парламента, почетком 2010. године, у свету су постојала 134 сателитска система за прислушкивање. Једина земља која контролише све јесте Америка која преко глобалне обавештајно-сателитске организације „Vortex“ (основане 1947. са Енглеском) и анализе највеће шпијунске организације Ен-Ес-Ај прибавља скоро 70% обавештајних података. У Форт Миду, градићу државе Мериленд, налази се главни штаб ове мистичне установе која, запошљавајући 38.000 службеника, представља очи и уши електронско-обавештајне агенције.

„Много тога се променило од када смо могли да негирамо да ова агенција постоји, а смео бих да додам да је било председника који нису ни знали за постојање ове институције, мада су њене услуге и те како користили“, изјавио је Роберт Стил, директор ове мамутске компаније („Washington post“, 11. 12. 1999). Неки аналитичари су поборници теорије да је ова служба ефикаснија од служби ЦИА или Еф-Би-Ај, што донекле оправдава и њено учешће у свим ратовима у последњих неколико деценија. Постоји и велики број европских сарадника на овом плану, међу којима је највећи Велика Британија, а коју следе и Немачка, Француска, Аустрија и Турска. Супертајни систем „Ешалон“ стациониран у Глочестеру, у Великој Британији, контролише целокупан европски простор. За комуникације на Пацифику одговоран је прислушни центар Јакима. Станице у Норвешкој и на Кипру под директном су контролом НАСЕ, а ради смиривања светске јавности званично се баве „економском“, а од недавно и „антитерористичком“ шпијунажом. „Ешалон“ има 120 сателита и близу 1,320 моћних компјутера-речника, што му омогућава да прислушкује све војно-обавештајне и политичке комуникације широм Европе и света.[5]

Контрола је појам који ће у будућности доминирати светом, што доводи у питање слободу сваког појединца. САД су формирале специјалну јединицу за насилну неутрализацију страних медија, па стручњаци при генералштабу „US Strategic Command“, у ваздушној бази Офут, у Омахи, имају посебна задужења из области масовног комуницирања и пропаганде. Систем Превентивна контрола путника, успостављен договором Европске комисије и америчких власти посредством компјутера, проверава идентитет сваког грађанина, обележавајући га зеленом (безопасан), жутом (сумњив) и црвеном (опасан) бојом. У том смислу није се много одмакло од времена нацистичке Немачке, само што се грађани данас „обележавају“ невидљивим тракама, а посебна пажња обраћа се на муслимане или особе чије је порекло са Блиског истока.

[5] Schmit, M., N., *CAN and the jus in bello: An introduction*, K. Bustrom, op. cit. 2005, pp. 17.

Сједињене Америчке Државе су у своје картотеке, без знања и одобрења њихових влада, увеле 75 милиона Мексиканаца, 42 милиона Колумбијаца и 33 милиона Централноамериканаца. Параноје нису поштеђени ни амерички држављани, па је тако враћен низ ретроградних закона који доводе у питање и приватност и слободу људских права.[6]

У свету нарастајућих подела и разлика у једном смо исти – сви смо конзументи различитих информација. Медији стварају технолошки парадокс – што више телевизијских програма, штампаних листова и часописа, радио-станица или интернета – мање слободног времена. Тако смисао живота постају похлепа и задовољавање све ширих потреба, док цивилизацијски однос ка култури и степену задовољавајуће комуникативности нестаје у мору нарастајућих хедонистичких захтева. Тоталитаризам искључује слободу изражавања, развој критичке мисли и супротстављеност аргументације, док демократија почива на медијима, како би процес владања био отворен широкој јавности. Нова цивилизација почива на свету слика, које често, ради стварања имица, могу бити медијски обликоване лажи. Основна и најважнија разлика између производа човека (творца) и осталих биолошких врста јесте што је човек средиште симбола који се судбоносно могу уплитати у целокупни фонд духовних потреба. Интелектуални, моралан човек новог поретка будућност темељи на размишљању и избору мњења, уз уважавање Монтескијеове мисли: „Политичка слобода никако се не састоји у томе да свако ради шта хоће .... Слобода је право да свако ради оно што закони дозвољавају."

Демократске структуре не могу опстајати без слободних, економски независних медија, при чему се не треба заваравати представом да је стварање повољне политичко-економске климе лак посао. Прецизна, тачна, умивена и професионална информација развија позитивне вредности неког друштва, фаворизујући људе који доносе опште добро. Без медија данас нема било каквог масовног комуницирања, тако да, поред класичног поимања о њиховој важности за развој културе, образовања и очувања националног идентитета, добијамо стратешку димензију учесника у процесима демократског преображаја друштва. Уместо некадашње четврте, пете или седме силе, новинарство данас постаје прва моћ, без чијег постојања нема друштвеног напретка.

Бурне друштвене и технолошке промене на размеђу миленијума дале су медијима нову значењску димензију, активно их промовишући у учеснике динамичких глобалних процеса. Брзина одлучивања, покретљивост становништва, уз ширење индивидуалних и потрошачких вредности, мењају традиционалне облике комуницирања, али и однос ка информацијама, чија се вредност посредством масмедија све више инструментализује.

Савремена средства комуникације на бази нових технологија стварају квалитативно нови облик комуницирања: мултимедије који мењају начин стварања, дистрибуције, ширења и складиштења информација. Као неминовност проистиче интегративно-регулативна функција, која практично одржава хомеостатичку стабилност читавог друштва, управљајући њиме. Бујање и пролиферација електронских и дигиталних канала дистрибуције порука ствара нову публику, која ће протоком времена све више зависити од дотока информативних, забавних или едукативних садржаја.

[6] Nešković S., Ikonomičeskata diplomacija v konteksta na nacionalnata i globalnata sigurnost, Veliko Trnovo, Bugarska: Univerzitet Sv. Kiril i Metodij, 2011, str. 91.

Интелектуални инжењеринг опстаје на знању и вештинама, при чему је економска моћ нераздвојиво повезана са политиком. Моћ знања и моћ савести су стубови коректног новинарства, али под притисцима медија да испуне захтеве тржишта новинари често долазе у сукоб са сопственим идеалима. Медијско друштво добија своје гладијаторе, нове терористе, који укидајући просторне и временске границе диктирају пожељне ставове и јавно мњење. Дигитална економија представља изазов за медије, тако да само врхунским познавањем њене структуре можемо спречити манипулисање. Захваљујући техничким проналасцима повећана је пропусна моћ медија, нпр. оптичко влакно може истовремено пропустити преко милион телевизијских канала, 200 хиљада пута брже од бакарних парица. У блиској будућности предвиђа се пренос сигнала ваздухом, што поред слободе дистрибуције значи и огромну компресију података. Корисници ће на тај начин добити веће богатство избора, наравно уколико буду у стању да то финансијски испрате.

Овакве технологије утемељене су на системима за дигитално емитовање звука и слика није нимало наивна, јер са собом носи читав низ важних унапређења, као што је једнофреквентна мрежа телевизија високе дефиниције и вишеканално емитовање.[7]

Прелаз од природе ка техносфери одвија се уз помоћ информатичких мрежа, што само појачава опасност кондиционирања мишљења, потреба, ставова, вредносних система, облика контроле и сл. Колективно понашање усмерава се према потребама медијских императора, па тако можете провоцирати масовну хистерију, халуцинације, побуне, демонстрације, гласине, митове, али и оптимизам, задовољство, спектакл, легенде и сл.

Нова цивилизација негује нове медије који постају произвођачи милиона вести, а умножавањем канала и садржаја стварају деперсонализоване јединке подложне манипулисању. Нове технологије стварају нове сензибилитете, пре свега филозофију мондијализма, чудесну у настојањима унифицирања идеја и система вредности. Дигиталне технике мењају карактер стандардних комуникација, њихових облика и величина. Минијатуризација опреме омогућава да технолошким спојем камере, телевизије, компјутера и телефона, у сваком тренутку и са сваког места, можемо бити укључени у програме информативних кућа.

Произвођачи електронске опреме већ усавршавају прототип телевизијског екрана од течног кристала, са специјалном поларизацијом светлости, тако да када је апарат у мрежи посматрате слику, а док је искључен представља обично огледало. Кориснику се нуди читав низ могућности, да, на пример, део екрана користи за огледало, а да истовремено на остатку гледа и најновије вести.

Повезивањем са компјутером омогућава се двосмерни пренос хируршке операције и експертског тима који то надгледа са више стотина километара удаљености или другог краја планете. Мултимедијално обликовање порука дубоко нарушава психолошко-пропагандне обрасце, јер се технолошком изменом човекове околине и сами мењамо.

Противречности добрим делом проистичу из злоупотребе природе медија, политике и јавног мњења, при чему је мање битно колико су механизми контроле покривени. Нови комуниколошки поредак представља отворен концептуални оквир у

[7] Милашиновић С., Јевтовић, З., Деспотовић, Љ., Политика, медији, безбедност, Београд: Криминалистичко-полицијска академија, 2012, стр. 125.

којем предност имају технолошки развијеније државе.[8] Схватања да се тежиште утицаја пребацује на медије локалних заједница само се делимично тачна, јер је њихов домет ограничен, што уједно значи и моћ на мишљење публике. Они олакшавају убеђивање и дијалог у оквиру мањих група, али су на ширем плану стратешки безначајни, па не треба беспотребно расипати средства на њихов развој.

Прве институције које су извршиле транзицију ка приватизацији нимало случајно били су медији, како по власништву, тако и по садржају. Амерички капитал је највећим делом помагао независност у Пољској, Мађарској, Чешкој, Србији и другим комунистичким земљама, што се објашњавало процесима демократизације и одбране медијске независности.

Наша јавност споро схвата дубину медијских промена, па се тако још увек носи заблуда да су новинари „занатлије" којима факултетско образовање није потребно, посебно ако су „талентовани". Између појмова занимање и професија дубок је јаз неразумевања. У САД се више не поставља питање потребе њиховог образовања, јер се на време схватило да нове технологије, мењајући филозофију медија и друштва, захтевају виши ниво знања. Комунистички стереотипи о новинарима као универзалним незналицама, друштвено политичким радницима и слично доказ су инструментализације позива. Време је да схватимо да знање у погрешним рукама или главама никада није корисно.

Глобализована конфигурација међународне заједнице

Међународни односи и њихов нормативни оквир међународног права одраз су Вестфалског система суверених држава. У том систему територија је један од конститутивних елемената, па не чуди што је представљала и представља једну од основних вредности међународних односа и међународног права. Развој технике и технологије ширио је простор који се сматрао државном територијом. Научна достигнућа 20. века отворила су пролаз у четврту, виртуелну димензију. У међународним односима устоличен је нови извор моћи – информација. Она није више само средство, већ циљ, вредност коју треба заштити и од које зависи безбедност државе и њених становника, вредност због које ће се ратовати.

Међународно право је екскомуницирало рат између међународних односа након Другог светског рата. Механизам који омогућава друштву да изабере своју будућност уредио је међународне односе на начелу забране, претње силом и употребе силе. То не значи да су ратови нестали као облик међудржавних односа. Штавише, они су се трансформисали и усложили, пратећи промене на међународној сцени. Међународно право поседује сопствени механизам и омогућава да се овлада реалношћу. Механизам који се активира када је будућност друштва угрожена, јер је сила употребљена, и који ограничава силу у мери у којој је друштву неопходна да би опстала и опоравила се назива се међународно хуманитарно право.[9]

[8] Исто, стр. 127.

[9] O Donneli, B., T., Kraska, J., C., *Humanitarian law: developing international humanitarian rules for the digital battlefield*, Journal of Confict and Security Law, Vol 8, No. 1, 2003, pp. 10.

Иако су многи склони закључку да је употреба информационих технологија променила ток ратовања, то није истина. Природа рата се није променила. Рат је и даље наставак политике другим средствима. Оно што се променило је начин његовог вођења. Информационе технологије омогућиће будућим армијама да раде оно што су армије одувек радиле, али успешније него раније. Да би разумели утицај информационих технологија и испитали адекватност правила међународног хуманитарног права изазовима револуције у војним пословима морамо променити угао гледања, јер ми на рат још увек гледамо као на сукоб држава са традиционалним оружјима која производе смрт или уништење опипљивих објеката и физички прелазак националних граница.

Наш први задатак је да опишемо и именујемо појаве које одликују нови начин ратовања. Први појам с којим се упознајемо јесу информационе операције. То су акције које се предузимају како би се утицало на противничке информације и информационе системе, истовремено бранећи сопствене информације и информационе системе. Посебан вид информационих операција јесте информационо ратовање. То су акције које се предузимају како би се током периода криза или рата постигла информациона супериорност путем утицаја на непријатељске информације, процесе засноване на информацијама, информативне системе и компјутерске мреже. Информационо ратовање одредили смо као посебан тип информационих операција. На основу оваквог одређења логично је претпоставити да право које регулише оружане сукобе регулише и овај вид ратовања и његове посебне форме, као што су напади на компјутерске мреже.[10]

Напад на компјутерске мреже представља операцију која за циљ има информације у компјутерима или компјутерским системима или саме компјутере или системе. Основни принцип који регулише вођење непријатељства у оружаним сукобима је принцип дистинкције. Он налаже странама у сукобу да у свако доба праве разлику између цивилног становништва и борца и између цивилних објеката и војних објеката и да, сходно томе, усмере своје војне операције само против војних објеката. Напад на компјутерске мреже, како смо већ истакли, представља операцију која има за циљ информације у компјутерима или компјутерским системима или саме компјутере и системе.

У савременом друштву функционисање свих сектора, па и војних, све више зависи од информационих технологија. То је посебно случај са тзв. критичним инфраструктурама, инфраструктурама које су од посебне важности за функционисање савремених друштава, а истовремено су веома повезане и међузависне. Информационе инфраструктуре представљају укупност повезаних компјутера и мрежа и битних информација које се њима прослеђују. Повезаност војног и цивилног сектора друштва путем информационих инфраструктура представља посебну погодност за извођење CNA – нападима на компјутерске мреже (computer networks attacks). Значај информације за нормално функционисање компјутерских система у свим секторима савременог друштва упућује на могућност укључивања информације у домен дефиниције војног циља. Наиме, војни сектор данас се све више ослања на информационе технологије цивилног сектора, јер су они јефтинији и доступнији.

[10] Милашиновић С., Јевтовић, З., Деспотовић, Љ., стр. 131.

Конфликти су по својој садржини променљиве, динамичне, вишеструко узроковане и сложене друштвене појаве. Њихови најдубљи корени налазе се у противречности и супротности између интереса, вредности или значајних ресурса (материјалних и духовних) којима желе располагати носиоци конфликта. Наш задатак је да опишемо и именујемо појаве које одликују нови начин ратовања. Први појам са којим се сусрећемо јесте информациона операција (Information operation). То су акције које предузимамо како би утицали на противничке информације и информационе системе. Оне се изводе и у доба мира и у доба рата. Офанзивне информационе операције утичу на противничко одлучивање, док дефанзивне утичу на спречавање извођења информационих операција на пријатељске снаге и вредности.[11]

Оно што их одликује нису средства која се употребљавају, већ ентитет на који се утиче, тј. информација. Посебан вид информационих операција јесте информационо ратовање (information warfare). То су акције које се предузимају како би се током периода криза или ратова постигла информациона супериорност путем утицаја на непријатељске информације, процесе засноване на информацијама, информативне системе и компјутерске мреже. Америчко ваздухопловство прецизира поделу информационих операција на информационо ратовање и ратовање у информацијама.

Информационо ратовање обухвата акције напада и одбране информација и информационих система, док ратовање у информацијама обухвата акције прикупљања и коришћења информација. Информационо ратовање смо одредили као посебан тип информационих операција које се изводе током оружаних сукоба или криза. На основу оваквог одређења логично је претпоставити да право које регулише оружане сукобе регулише и овај вид ратовања и његове посебне форме. У посебне форме могу се убројати напади на компјутерске мреже.

Правила међународног хуманитарног права упутила су доктрину да одреди генеричку дефиницију оружаног сукоба: „Оружани сукоб представља несагласност страна у сукобу која је довела до организоване употребе оружаних снага.[12] Међународно хуманитарно право разликује два типа оружаних сукоба, међународне и немеђународне оружане сукобе. Дихотомија одређује који део корпуса међународног хуманитарног права се примењује у овим ситуацијама.

У овом раду фокусираћемо се на најстарији тип оружаних сукоба који регулише тај корпус права – сукобе између држава. Најзначајнији формални извори права који регулишу овај тип међународних оружаних сукоба су Женевске конвенције о заштити жртава рата (1949) и њихов први допунски протокол (1977), а користићемо их као аналитички оквир овог истраживања. Заједнички члан 2. Женевских конвенција (1949) одређује да међународни оружани сукоб постоји у случају објављеног рата или сваког другог оружаног сукоба који избије између двеју или више високих страна уговорница, чак иако једна од њих није признала ратно стање.

[11] Schmit, M., N., CAN and the jus in bello: An introduction, K. Bustrom, op. cit. 2005, pp. 102.

[12] Међународни оружани сукоби обухватају сукобе између држава и ситуације војне окупације (чл. 2. Женевска конвенција) и оружане сукобе у којима се народи боре против колонијалних или расистичких режима или стране окупације користећи се правом на самоопредељење. Немеђународни оружани сукоб настаје када на територији једне државе дође до употребе оружаних снага владе против побуњеног дела оружаних снага или неке организоване оружане групе или када се сукобљавају различите организоване наоружане групе (чл. 3. Женевских конвенција, чл. 1(1) Протокола II).

У савременом друштву функционисање свих сектора, па и војних, све више зависи од информационих технологија. То је посебно случај у такозваним критичним инфраструктурама, инфраструктурама које су од посебне важности за функционисање савремених друштава, а истовремено су веома повезане и међузависне.

Информационе инфраструктуре представљају укупност повезаних компјутера и мрежа и битних информација које се њима прослеђују. Значај информационих инфраструктура је у томе што се њиховим онеспособљавањем може онемогућити функционисање свих осталих критичних инфраструктура.[13] Посебно су значајне информационе инфраструктуре које надзиру и контролишу битне друштвене функције и услуге (дистрибуцију електричне енергије, телекомуникације, банкарске информације и услуге, контролу железничког и авио саобраћаја, системе за ванредне ситуације, берзу и контролу безбедности).

Дефиниција војног циља упућује на предмете – објекте. CNA има за циљ информације или компјутерске системе. Материјални објекти у којима је информација складиштена или пут којим се она прослеђује несумњиво представљају потенцијални војни циљ. Доктрина сматра да само материјалне, опипљиве ствари могу представљати војни циљ.

Значај информације за нормално функционисање компјутерских система у свим секторима савременог друштва упућује на могућност укључивања информације у домен дефиниције војног циља. Информација се може користити тако да ефикасно доприноси војној акцији стране у сукобу. Ефикасан допринос подразумева постојање блиске везе са војном акцијом. Из његовог домена искључени су посредни доприноси, тј. доприноси свеукупном ратном напору. Ово ограничење је веома битно за регулисање CNA. Идеје о утицају информационих технологија на проширење спектра војних циљева засноване су на либералнијем тумачењу дефиниције војног циља, тумачењу које потиче из редова америчких оружаних снага. Њихови документи истичу да је кључни фактор у избору мете напада да ли објекат доприноси непријатељским борбеним капацитетима или капацитетима за одржавање рата.[14]

Као илустрацију наводимо пример из америчког грађанског рата, када су снаге Севера уништиле поља памука на територији Југа, јер се од продаје памука финансирало наоружавање њихових оружаних снага. Повезаност војног и цивилног сектора друштва путем информационих инфраструктура представља посебну погодност за извођење CNA.

Данас се војни сектор све више ослања на информационе технологије цивилног сектора, јер су и јефтинији и доступнији. Оружане снаге користе ЦОТС, односно комерцијалне хардвер и софтвер производе, који служе за обављање административних послова, али и у системима за извођење напада у оружаним сукобима, с обзиром на чињеницу да су ови производи намењени углавном за цивилну употребу, опремљени су слабим заштитним механизмом.

Многи од тих софтверских и хардверских компоненти не производе се у земљи већ у иностранству, тј. код потенцијалних противника, што може представљати додатни проблем. Примера ради, војни и цивилни сектор заједнички употребљавају сателитске телекомуникације – INTELSAT, EUROSAT, ARABSAT, па би напад на

[13] Милашиновић С., Јевтовић, З., Деспотовић, Љ., стр. 136.

[14] U. S. Department of Navy, Naval Warfare Pub 1–14 M, The Commanders Handbook on the Law of Naval Operations, 1995, para, 8.1.1., U. S. Department of Air Forc Pam. 14–210. U. S. Air Force Targeting Guite, 1998., para, 1.7.

компјутерске системе који их регулишу произвео проблеме у функционисању контроле авио саобраћаја, односно сударе или падове авиона. Такође, напад на компјутерске системе који контролишу електричну мрежу која напаја симултано и војни и цивилни сектор, довео би до пада система за пречишћавање и дистрибуцију воде или система напајања болничких апарата, што даље доводи до цивилног губитка.

Мере предострожности представљају активности које су стране у сукобу дужне да предузму како би се избегли или ограничили цивилни губици током напада на војни циљ. Лице које планира или одлучује о нападу прво предузима све могуће мере предострожности да потврди да је одабрана мета напада војни циљ. Наиме, међународно хуманитарно право забрањује нападе на цивиле и цивилне објекте, као и на објекте који су под цивилном заштитом. Реч је о објектима као што су културна и духовна добра, објекти неопходни за опстанак цивилног становништва, грађевина и инсталације које садрже опасне потенцијале, природна средина и санитетске јединице и транспортна средства. Друга обавеза лица која планирају напад или одлучују о њему јесте да предузму све могуће мере предострожности при избору средстава и метода напада ради избегавања или минимизирања ненамерних цивилних губитака.

Иако су се за извођење непријатељства користила и користе првенствено кинетичка оружја, међународно хуманитарно право регулише и употребу других врста оружја. На почетку 20. века забранило је употребу загушљивих отровних и других сличних гасова и бактериолошких течности или материја, а у другој половини регулисало је забрану употребе, развоја, ширења, транспорта, складиштења и начин уништења биолошког и хемијског оружја. Осим тога, у члану 36. Протокола I изричито је истакнуто да „у проучавању, усавршавању, набављању или прихватању новог оружја, средстава или метода ратовања висока страна уговорница је обавезна да утврди да ли ће његова примена, у неким или свим условима, бити забрањен Протоколом или неким другим правилом међународног права које се примењује на високу страну уговорницу".

Имајући у виду природу CNA, можемо рећи да информација представља оружје које носи огроман позитиван потенцијал. Може омогућити остварење војне предности без жртава.[15] Међутим, негативан потенцијал информације као оружја у могућој је индискриминативној употреби. Међународно хуманитарно право забрањује употребу оружја чија се дејства не могу усмерити на одређени војни циљ, већ погађају војне циљеве и цивилне објекте без разликовања. Нападач може креирати вирус који након убацивања у војну компјутерску мрежу наставља неконтролисано да се шири и на цивилне информационе системе.

Према међународном хуманитарном праву забрањено је убијати, рањавати или затварати противника, прибегавајући перфидним поступцима. Замислимо да припадник оружаних снага прими наизглед сасвим безопасан имејл за који претпоставља да је од цивилног пошиљаоца, а који у датотеци садржи вирус. То може бити пример злоупотребе цивилног статуса. Такође, информације се могу користити и како би се противникова борбена средства приказала као санитетска. У литератури се користи и пример коришћења компјутерских кодова и мрежа да би се емитовао лажни снимак председника противничке државе, где он обавештава припаднике

[15] Hslam, E., *Information warfare tehnological changes and international law*, Journal of Conflict and Security Law, Bol 5, No. 2, 2000, pp. 14.

својих оружаних снага да је склопљен мир и да се предају. Овакав поступак представљао би виртуелни еквивалент злоупотреби заставе примирја или предаје.

Примери ратних лукавстава су: коришћење камуфлаже и мамаца, лежне операције и погрешне информације. Лице које планира или одлучује о CNA не сме да користи забрањене методе и средства за извођење напада и дужно је да изврши селекцију између доступних правно дозвољених средстава напада. Прво је дужно да изабере средство напада, односно онај тип компјутерског кода који ће омогућити избегавање цивилних губитака током напада на војни циљ. У условима CNA то би значило да бира средство које неће имати последице по функционисање компјутерских система цивилних инфраструктура. Ако то није могуће, одабраће средство које последице своди на минимум. У случају да се на овакав начин не могу ограничити последице напада на војне компјутерске мреже, лице које планира или одлучује о CNA провериће да ли се као последица CNA могу очекивати цивилни губици који би били несразмерно велики у односу на предвиђену конкретну и директну војну предност.

Битно је истаћи две напомене. Прво, принцип пропорционалности не односи се на губитке који су последица директног намерног напада на цивиле. Забрана ових напада регулисана је принципом дистинкције и не може се дерогирати позивањем на војну потребу. Друго, утврђивање пропорционалности је прогностички задатак. Принцип пропорционалности не односи се на стварне, већ на очекиване цивилне губитке. Будући да CNA може проћи без примарних цивилних губитака, чини нам се да у условима међузависности цивилног и војног сектора од идентичних информационих система и секундарне последице укључимо у домен теста пропорционалности.

Ако се зна да је компјутерски систем који представља војни циљ умрежен са системима који контролишу критичне цивилне инфраструктуре може се очекивати да ће такав напад проузроковати секундарне или кумулативне цивилне губитке који би били несразмерно велики у односу на војну предност која се може предвидети као резултат CNA.

Војна предност мора бити конкретна, тј. одређена и опажљива. Такође, мора бити и директна, тј. да се остварује без уплитања посредних фактора. Одлике војне предности наведене у дефиницији војног циља и формулацији члана 57(2)(а) Протокола I указују да се може говорити само о тактичком плану, никако о стратешком. Функционална повезаност информационе инфраструктуре различитих сектора друштва усложила је ионако тежак задатак процене пропорционалности напада. Процена пропорционалности CNA захтева експертско познавање информационих технологија које не одликује војне планере или одлучиоце.

Ради избегавања или ограничавања цивилних губитака током CNA, страна у сукобу је дужна да изврши селекцију војних циљева који нуде сличну војну предност. Одабраће се онај војни циљ од чијег уништења се очекује да ће произвести најмању опасност по цивилно становништво. У случају да постане јасно да CNA није усмерен на војни циљ или да ће проузроковати непропорционалне цивилне губитке, поништиће се одлука о нападу или, ако је он већ започет, прекинуће се.

Као допунски механизам за заштиту цивила током CNA можемо идентификовати упозорење о нападима који могу угрозити цивилне компјутерске или системе цивилне инфраструктуре. Да бисмо резимирали кораке које би одговорна лица требало да предузму у извођењу CNA, можемо искористити матрицу коју су понудили О Донели и Краска.[16]

[16] O Donneli, B., T., Kraska, J., C., Humanitarian law: developing international humanitarian rules for the digital battlefield, Journal of Confict and Security Law, Vol 8, No. 1, 2003, p. 159.

Они су представили следеће нивое анализе легалности CNA:

– Који систем је мета напада и како функционише?

– Како ће напад утицати на систем који је мета напада?

– Које су директне последице напада?

– Који су системи интегрисани или повезани с мрежом која је предмет напада?

– Какве ће последице напад произвести на мреже које нису мета напада или повезане системе?

– Који су домино ефекти напада?

CNA може извести квалификовани припадник оружаних снага или било који становник Земљине кугле који поседује рачунар и приступ интернету. Доступност информационих технологија омогућило је стварање огромне „армије сајбер ратника" која се може употребити у оружаним сукобима за постизање информационе супериорности над непријатељем.

Примера ради, кинески хакери су на НАТО бомбардовање кинеске амбасаде у Београду 1999. године одговорили координираним нападима на компјутерске системе НАТО-а. Применимо услове за статус борца у условима CNA. Први је организованост. Она подразумева колективни карактер борби које се воде под одговарајућом контролом и према одређеним правилима, насупрот појединцима који делују изоловано без одговарајућих припрема или тренинга.

Савремене војне послове одликује све веће ангажовање цивила – специјализованих стручњака. CNA је пример ангажовања ИТ стручњака. Ако су инкорпорирани у састав оружаних снага они ће имати статус борца/ратног заробљеника. Ако су унајмљени за обављање специјализованих ИТ послова њихова заштита од напада зависиће од врсте активности које обављају. Ако њихов ангажман досеже праг директног учешћа у непријатељствима, они ће представљати легалну мету напада.

Одређена питања о примењености међународног права на CNA остају отворена. То не значи да међународно хуманитарно право не може адекватно да одговори изазовима међународног ратовања. Нова димензија и нов начин ратовања не подразумева нужно и ново право. Они захтевају разумевање нових технологија, јер је појединац суочен с правом које разуме и са технологијом коју не разуме, често пре спреман да прихвати да мења право неголи да се потруди да разуме технологију.

Закључак

Економска шпијунажа представља прворазредни инструмент за постизање компетитивне предности компанија, унапређење националне економије и реализацију државних интереса сваке земље у међународној заједници. У савременом амбијенту носиоци процеса глобализације користе све легалне, али и нелегалне, најчешће нехумане методе и поступке деловања на светском тржишту у контексту остваривања пројектованих циљева. Међународна економска шпијунажа представља софистицирану област деловања субјеката међународне заједнице у условима глобализације.

Једна од приоритетних делатности у којима државе и њени субјекти остварују компетитивну предност на светском тржишту јесте економска обавештајност, односно способност располагања релевантним информацијама. Захваљујући добро орга-

низованим институцијама и оспособљеним ресурсима у сфери економске шпијунаже, одређена земља може реализовати пројектоване спољноекономске циљеве и обезбедити значајне ефекте за сопствену заједницу. При томе је битна конкретна стратегија деловања свих органа државе на унутрашњем и међународном плану.

Имплементација концепта међународне економске шпијунаже заснива се на примени нових технологија у информационо-комуникационој сфери. Револуционарни напредак у информационој и комуникационој технологији има два истовремена и комплементарна утицаја на земље у развоју. Прво, отварају изванредне могућности за убрзање друштвеног и економског развоја. Друго, стварају нарастајућу потребу за реформом политике и инвестирања, како би се искористиле нове могућности и избегло опадање међународне конкурентности.

Значај информационих инфраструктура је у томе што се њиховим онеспособљавањем може онемогућити функционисање свих осталих критичних инфраструктура. Посебно су значајне информационе инфраструктуре које надзиру и контролишу битне друштвене функције и услуге (дистрибуцију електричне енергије, телекомуникације, банкарске услуге, контролу железничког и авио-саобраћаја, система за ванредне ситуације, берзу и контролу безбедности).

Повезаност војне и цивилне инфраструктуре представља велику потенцијалну опасност за заштиту цивилног становништва и цивилних објеката током CNA. Напад на војне компјутерске мреже (које представљају легалан војни циљ) може произвести погубне последице по функционисање критичних цивилних информационих система, односно може резултирати цивилним губицима.

Основни принцип јесте забрана употребе средстава и метода који проузрокују сувишне повреде или непотребне патње. Одредбе и принципи међународног хуманитарног права захтевају коректно поступање у свим фазама одвијања конфликта, као и утврђивање природе повреде или интензитета патње у односу према војној употреби. С тим у вези потребно је утврдити да ли повреде или патње материјално превазилазе степен који је оправдан предвиђеном војном предношћу. Релевантни субјекти у постмодерној конфигурацији међународног система имају обавезу да савремене технологије инкорпорирају у сврси обезбеђења просперитета људске популације.

Литература

1. Dedijer, S.: *Development and Management by intelligence/Japan,* 1991.

2. Luttwak, E.: *From Geopolitics to Geo-economics,* The national interest, 20, 1990.

3. Милашиновић, С., Јевтовић, З., Деспотовић, Љ.: *Политика, медији, безбедност*, Криминалистичко-полицијска академија, Београд, 2012.

4. Нешковић, С.: *Национални интерес и заштита животне средине у постмодерном глобалном амбијенту,* Факултет организационих наука, Београд, 2007.

5. Нешковић, С.: *Глобална безбедност у постмодерном амбијенту-импликације на националну безбедност и животну средину,* књига I, АПЕИРОН, Бањалука, 2009.

6. Нешковић, С.: *Икономическата дипломација в контекста на националната и глобалната сигурност*, Универзитет Св. Кирил и Методиј, Велико Трново, Бугарска, 2011.

7. O Donneli, B., T., Kraska, J., C.: *Humanitarian law: developing international humanitarian rules for the digital battlefield*, Journal of Confict and Security Law, Vol 8, No. 1, 2003.

8. Петровић, З. П.: *Економска шпијунажа: мали водич кроз историју економске обавештајности, до десете револуције човечанства,* Драслар партнер – Центар Југоисток, Београд, 2005.

9. Schmit, M., N.: *CAN and the jus in bello: An introduction*, K. Bustrom, op. cit. 2005.

10. U. S. Department of Navy, Naval Warfare Pub 1–14 M, *The Commanders Handbook on the Law of Naval Operations*, 1995, para, 8.1.1., U. S. Department of Air Forc Pam. 14–210. U. S. Air Force Targeting Guite, 1998., para, 1.7.

11. Hslam, E.: *Information warfare tehnological changes and international law*, Journal of Conflict and Security Law, Bol 5, No. 2, 2000.