ИНФОРМАЦИСКА БЕЗБЕДНОСТ ВО САД

Ванчо КЕНКОВ

355.45:004.056

АПСТРАКТ

Во современото општество информацискатa безбедност е компонента на националната безбедност. Во склоп на објаснувањето на поимот безбедност и поимот информациска безбедност дадени се основните поставки на општата наука за безбедност и теориите на информацискoто војување. Информацискатa безбедност се јавува не само како еден од облиците на бездбедноста, туку и како пресек на сите облици на безбедност во кои информатичките технологии заземаат важно место. Во тој контекст прикажан е односот на информацискатa, економскатa и воената безбедност и начинот на заштита на информацискатa инфраструктура на САД.

Клучни зборови: Безбедност, информациска безбедност, информациско војување, информациски операции, информациско обезбедување, заштита на информацискатa инфраструктура.

ABSTRACT

In the modern world, the IT security has grown into a part of the general concept of national security. The article argues that the parameters of the theory of information warfare arise from the fundamental postulates of the general theory of security. The information security is not only one more aspect of security as such but it is an essential part of all other forms of security where informative technologies have their say. In this context, the author elaborates the relationship between information, economic and military security and the manner in which the US have established and protected their information infrastructure.

Key words: security, information security, information warfare, information operations, protection of the information infrastructure, USA

Вовед

Еден од основните мотиви на човековата дејност и на општеството разгледуван низ историјата и, несомненео, еден од глобалните проблеми на современата епоха е безбедноста. Воопшто, до неодамна проблемот на безбедноста подразбираше анализа, пред сè, од воен аспект. Информациската безбедност, како еден од новите правци на истражување во сферата на безбедноста, се јави како последица на појавата и развојот на инфромациското општество. За значењето на информациската безбедност говори и фактот дека таа е една од основните компоненти во доктрините на националната безбедност на некои земји. Целта на овој труд е да покаже, на примерот на САД, дека информациската безбедност во современото општество е неодвоив дел од проблематиката на националната бебзедност и дека претставува една од основните компоненти.

Поим, содржина и суштина на информациската безбедност во САД

Поимот информациска безбедност во САД, односно информациското обезбедување е изведен и заснован на теоријата за информациското војување (IW *information warfare*). Иако, импилицитно не е наведено, исходиштето на теоријата за информациското војување е општата наука за безбедноста. Имено, по аналогија со електромагнетскиот спектар во чиј домен се одвива електронското војување (*electronic warfare*), американските воени експерти, во настојувањата да ги дефинираат револуционерните промени во воените дејности, информацискиот спектар го назначија како домен во кој се одвива информациското војување.

Теоријата на IW подразбира информациска доминација (концепт на информациска превласт, односно информациска супериорност). Информациската супериорност се реализира низ разузнавачко-набљудувачко-извидувачки операции, информациски менаџмент и информациски операции. Елемент за поддршка на информациските операции е информациското обезбедување.

Природа на информациите и информациското опкружување

Под поимот *информација* се подразбира податок кој е прибран од опкружувањето и обработен во форма која понатаму може да се користи[1], истата може да биде и содржина или значење на пораката[2]. Суштината на поимот *информација* произлегува од т.н.

[1] Field manuel No. 100-6, FM 100-6 *Information operations*, Deparment of the Army, Washington, DC, 1996.

[2] Maconachy V.,Schou C.,Ragsdale D., Welch D., *A model for Information assurance: an integrated approach,* Proceedingsof the 2001 IEEE, workshop on Information Assurance and Security, United States Military Academy, West Point, 2001.

когнитивна хиерархија, информацијата во голема мера, сама по себе е без значење, само кога податоците ќе се обработат, односно ќе се стават во ситуациски контекст, тогаш таа го добива своето значење и станува, по дефиниција, информација. Врз основа на информациите во процесот на спознавање настанува знаењето, тоа е информација која е испитана и прифатена како факт. Расудувајќи (размислувајќи) знаењето преоѓа во разбирање (на ситуацијата) со што се исполнуваат условите за донесување правилни одлуки (командантите, бизнисмените итн.)[3]. Оттука разликуваме системи на знаење и системи на верување. Системи на знаење се оние системи кои се организирани и водени да ги почувствуваат или перцепираат појавните индикатори кои можат да се верифицираат, да се преведат тие индикатори во разбирливи реалности кои се користат во донесувањето одлука или директна активност. Системите на верување се сите експлицитни емпириски податоци во форма на верификувани сознанија и сите други податоци кои не можат или тешко се верификуваат. Системите на верување, за разлика од системите за знаења, се изразито индивидуализирани и зависат од генетското наследство и културните традиции[4].

Релевантни информации се информации кои се одбрани од големо количество информации, а кои значително влијаат, придонесуваат или се однесуваат на извршување на дадена оперативна мисија[5].

Критериуми за проценка на квалитетот на информацијата се: *точност*-информации кои верно ја пренесуваат (претставуваат) ситуацијата, *релевантност* - информации кои се однесуваат на дадена мисија, задача или ситуација, *благовременост* - информации кои се на располагање кога треба да се донесе одлука, *целовитост* - сите потребни информации потребни на лице кое одлучува (донесува одлука), *прецизност* - информации кои во себе носат баран ниво на поединости (деталности).[6]

Битен поим во теоријата на IW е информациското опкружување. Информациското опкружување (*Informaiton Environment*) е целина, збир на поединци, организации или системи за собирање, обработка или дистрибуција на информациите[7]. Употребата на информации експоненцијално расте со развојот на општеството. Современото информациско опкружување се манифестира преку информациската структура. Разликуваме: глобална, национална и воена (GII, NII, DII, - *global national, defence information infrastructure, JP3-13, 1998*).

---

[3] Field manuel No. 100-6, FM 100-6 *Information operations*, Deparment of the Army, Washington, DC, 1996.

[4] Szafranski R., A theory of information warfare: preparing 2020, Airpower Journal, Spring, 1995.

[5] Field manuel No. 100-6, FM 100-6 *Information operations*, Deparment of the Army, Washington, DC, 1996.

[6] Исто

[7] Исто

Министерството за одбрана на САД и Одбранбениот научен борд (DSB – defence science board) имаат визија за остварување ефективна безбедносна архитектура да изградат интегрирана информациска инфраструктура (III – integrated information infrastructure), а станува збор за глобална информациска мрежа GIG (*global information grid*) која треба да ги исполни барањата на информациското обезбедување (IA): инфраструктура и апликација на јавниот клуч PKI и PKE, GIG IA тестирање DID архитектура (*defence- in-depth* - одбрана во длабочина) IP sec, IA функции, можност на менаџментот за безбедност на мрежата, линк енкрипција на физичко ниво на отворен модел и способност на преживување (*Protecting the Homeland, report of the Defence science board, 2001*).

Извори на закани се: хакери, инсајдери, активисти на анти-државни организации, терористи, странски учесници во информациските операции и информациски братоубијци, (несакани ефекти на сопствените или непријателски сили).[8] Методи на напади се: неутрализиран пристап, злонамерни програми, електро-магнетско дезинформирање или **мамење**, електронски напад и физичка деструкција[9].

Информациско обезбедување во концептот на информациското војување

Информациското војување начелно е опсег на акции кои се преземаат за да се оствари информациска супериорност над противникот. Во таа насока е и воената дефиниција која е дадена во CJCSI (*Chaiman of the Joint chief of Staff* - претседавач на здружениот генералштаб) 3210.01[10] со која информациско војување се дефинира како: активности кои се преземаат да се оствари информациска супериорност така што ќе се влијае на противничките информации, процесите засновани на информации, информациските системи и мрежи засновани на компјутери, додека во исто време ќе се пристапи кон одбрана на сопствените информации, процеси засновани на информации, информациските системи и мрежите засновани на компјутери.

Целта на информациското војување е да се оствари значителна информациска предност која би им овозможила на севкупните сили брзо да доминираат и да управуваат со противникот. Стратешката цел на IW е да се добие и одржи одлучувачка предност така што ќе се нападнат противничките информациски системи преку експлоатација, оневозможување и влијаење, а во исто време да се оствари заштита на сојузничките информациски системи.

---

[8] Field manuel No. 3-13, FM 3-13 (FM 100-6) *Information operations:Doctrine, Tactics, Technigues, and Procedures,* Deparment of the Army, Washington, DC, nov 2003.

[9] Исто

[10] Field manuel No. 100-6, FM 100-6 *Information operations*, Deparment of the Army, Washington, DC, 1996.

На Универзитетот за национална одбрана - NDU[11] работна дефиниција за информациското војување е пристап на вооружен конфликт кој се насочува на менаџмент и користи информации во сите облици и на сите нивоа за да се оствари одлучувачка воена предност, посебно во интервидовското и комбинираното опкружување. Информациското војување по природа е и офанзивно и дефанзивно и се движи од мерки со кои противникот се спречува да експлоатира информации до адекватни мерки со кои се обезбедува интегритет, расположивост и интероперабилност на пријателските информациски ресурси. Информациското војување иако во краен случај по својата природа е воено, се води и во политичката, економската и општествената сфера и е применливо преку голем спектар на националната безбедност од мир до војна.

Информациското војување може да се дефинира и како облик на конфликт со кој директно се напаѓаат информациските системи а со тоа и системите на знаење и верување на противникот.[12]

Мартин Либицки дава една поконкретна и поопиплива дефиниција за информациското војување според која, информациското војување, како посебна техника на војување, не постои, но постојат неколку различни облици на информациското војување:

– *војување во сферата на командувањето и управувањето* C^2W *(command end control warfare)* наменето за удари против „главата и вратот" на противникот;

– *разузнавачко војување IBW (Intelligence – based warfare)* насочено кон директна употреба на разузнавачките дејности за нишанење и врз целите и проценка на борбените дејства, реализација на концептот „стрелец-цел" ;

– *електронско војување* EW (*electronic warfare*) - опфаќа радио-електронски и криптографски техники;

– *психолошко војување* PSYW (*Psyhological wafare*)- информацијата се користи за промена на свеста на човекот;

– *хакерско војување* се напаѓаат компјутерските системи;

– *економско-информациско војување* EIW (*economic information warfare*) – блокирање или насочување на информациите за да се обезбеди економска доминација;

– *кибер војување* – збир на футуристички сценарија.

[11] National Defence University е највисока воено-политичка школа во САД и нејзини слушатели се покрај офицерите и високите службеници на администрацијата на САД, и офицери на други земји. Слушателите се примаат по покана а често и по име.

[12] Szafranski R., A theory of information warfare: preparing 2020, Airpower Journal, Spring, 1995

Оттука, информацијата сама за себе, не е медиум на војување, освен во најтесна смисла (електронско попречување). Крајната цел на информациското војување е информацискатa супериорност (IS – *information superiority)*, истата е дефинирана како оперативна предност добиена од можностите за собирање, обработка и непрекинат тек на дистрибуција на информациите при експлоатирањето или оневозможување на противникот да ги има истите можности (ФМ 3-0). Информацискатa супериорност се постигнува низ:

- информациски менаџмент (IM – *information menagament*);
- разузнавачка дејност, набљудување и извидување (ISR - *intelligence, surveillance and reconnaissance*);
- информациски операции (IO – *information operations*).

Основата на информацискатa супериорност се разузнавачката дејност, набљудувањето и извидувањето (ISR), а оттука американската воена доктрина ги дефинира ISR операциите. Поимот *информациски операциии* има претрпено значителни промени од првобитното дефинирање (ФМ 100-5, ФМ 100-6, 1996) до најновите сфаќања (ФМ 3-13, 2003). Промените пред сè се во содржината, односно во компонентите и можностите што ги прават IO. Друга суштинска промена е во фактот дека IO воедно се и елементи на борбените сили (combat power). Суштината на IO е дадена во Здружената доктрина за информациски операции (Joint Pub 3-13, Joint Doctrine for Information Operations, 1998) каде се вели: информацискатa операција вклучува активности кои влијаат на противничките информации и информациски системи при што единствено се заштитени сопствените информации и информациски системи.

Во одбарнбената доктрина на САД, информацискитe операциии имаат една од најважните улоги, што може да се потврди во *Air Force Doctrine Document 2-5* (information operations) каде се вели: доминацијата во информацискиот спектар денес е толку суштинска и важна, како превласта во воздухот или вселената или заземање територии во минатото, дека е согледана како неопходна и синергична компонента на воздушно-вселенската моќ (АФДД 2-5, 1998:5). Основни елементи на информацискитe операции се: јадро (core) на можности и можности кои ги поддржуваат - епизодни.

Покрај другото, информацискитe операции ги вклучуваат и јавните работи PA (*public affairs*) и цивилно-воените операции CMO (*civil-military operations*)[13]

[13] Field manuel No. 3-13, FM 3-13 (FM 100-6) *Information operations:Doctrine,Tactics,Technigues,and Procedures,* Deparment of the Army, Washington, DC, nov 2003.

Елементи (компоненти) на информациските операции[14]

Јадро		Кој ги поддржува	
Име		Име	
Електронско војување	EW	*Физичко уништување (physical destruction)*	
Операции поставени на комп. Мрежа (computer network operations)	CNO	*Информациско обезбедување (information assurance)*	IA
Напад на компјутерска мрежа (computer network attack)	CAN	*Физичка безбедност (physical security)*	
Одбрана на компјутерската мрежа (computer network defence)	CND	*Контраразузнавачка дејност (counterintelligence)*	CI
Експлоатација на комп. мрежа (computer network exploitation)	CNE	*Противзалажување (counterdeception)*	
Психолошки операции (psychological operations)	PSYH OP	*Противпропаганда (countederpropaganda)*	
Оперативна безбедност (operations security)	OP-SEC		
Воено залажување (military decception)			

Информациските операции можат да бидат офанзивни и дефанзивни (одбранбени). Офанзивните IO се дефинираат како интеграција за употреба на основните и поддржуваните можности и активности кои меѓусебно ја поддржуваат разузнавачката дејност, нападите на противничкото одлучување или влијаат и потпомагаат други специфични цели (FM 3-0). Информациските предности на IO се: уништување (*destroy*), прекинување (*disrupt*), деградација (*degrade*), одбивање (*deny*), залажување (*deceieve*), експлоатација (*exploit*) и влијание (*influence*)[15].

Одбранбените IO (DIO - defence IO) се дефинираат како интеграција и координација на политики и процедури, операции, на персона лот и технологијата за заштита и одбрана на пријателските информации и информациските системи. DIO обезбедува благовременост, точност и релевантност на информациите, а негови одбранбени елементи се: заштита (*protection*), детекција (*detection*), реставрација (*restoration*) и реакција (*response*). Одбранбените информациски операции користат технички и нетехнички актив-

[14] FM 3-13, 2003.

[15] Field manuel No. 3-13, FM 3-13 (FM 100-6) *Information operations: Doctrine, Tactics, Technigues, and Procedures,* Deparment of the Army, Washington, DC, nov 2003.

ности за ограничување на ранливоста на пријателските C^2 системи во непријателските информациски операции. Заедничката доктрина на информациските операции, информациското обезбедување го дефинира: информациското обезбедување е дефинирано како IO за заштита и одбрана на информациските системи обезбедувајќи услови за нивна расположивост, интегритет, доверливост и неодречивост. Сето тоа подразбира реставрација на информациските системи со инкорпорирани можности за заштита, детекција и реакција[16]. Термините расположивост, интегритет, автентичност, доверлиивост и неодречивост ги изразуваат целите на IA и се дефинирани како обезбеден пристап на авторизираните корисници, заштита од неавторизираните промени, верификација на оригиналноста, заштита од неавторизирани, обелоденување и неоспорен доказ за учество во извршените операции. Информациското обезбедување е специфична поткатегорија на информациските операции која ја покрива нејзината одбранбена област. Информациското обезбедување претставува континуиран процес кој го покрива целиот опсег на IO од мир, преку главниот судир до враќањето во состојба на мир. Особено истакнато значење на информациското обезбедување е дадено во Заедничката визија за 2020.

Заклучок

Во практиката и теоријата на националната безбедност, до неодамна се сметало дека најважна е воената компонента. Денес, очиглени се недостатоците на таквиот приод бидејќи научно-техничката револуција доведе до формирање на информациско општество во кое информацијата е главен фактор во управувањето со светот.

Технолошката револуција во областа на информациските и комуникациските системи услови промени во погледот на светот на почетокот на третиот милениум. Масовната компјутеризација и примена на новите информациски технологии доведоа до огромен напредок во сферта на масовните медии, бизнисот, индустриското производство, научните истражувања, образование, но, за жал, и во војувањето. Глобалните социјални промени, кои се последица на овие промени, бараат објективна анализа на формираната информациска средина на светската заедница. Проблемот на информацискатa безбедност, во досегашната историја, анализиран е само во контекст на заштита на информациите, пред сè, по пат на тотална физичка заштитеност и со разни ограничувања, што не можат да ги задоволат современите потреби. Информациското општество, кое со себе го носи третиот милениум, со себе носи нови закани, но и нови начини за нивно решавање.

[16] JP 3-13, 1998:1-9.

ЛИТЕРАТУРА

1. Field Manual No. 3-13, FM 3-13 (FM 100-6) *Information operations: Doctrine, Tactics, Techniques, and Procedures,* Deparment of the Army, Washington, DC, nov 2003.
2. Szafranski R., A theory of information warfare: preparing 2020, Airpower Journal, Spring, 1995
3. Field Manuel No. 100-6, FM 100-6 *Information operations*, Deparment of the Army, Washington, DC, 1996.
4. Maconachy V., Schou C., Ragsdale D., Welch D., *A model for Information Assurance: Aan Integrated Approach,* Proceedingsof the 2001 IEEE, Workshop on Information. Assurance and Security, United States Military Academy, West Point, 2001.
5. Field manuel No. 3-13, FM 3-13 (FM 100-6) *Information operations: Doctrine, Tactics, Technigues, and Procedures,* Deparment of the Army, Washington, DC, nov 2003.
6. Daniel G. Volf, *Statement before the House Select Committee on Homeland Security Subcommittee on Cyber-security, Science and Resarch & Development*, Nacional Security Agency US, july 22, 2003.
7. Вулета Вулетић, *Војна техника и војна доктрина*, ВИЗ, Београд, 2001.
8. Nacional Security Agency, *Nacional Information Systems Security Glossary*, NSTISSI No 4009, Fort Meade, MD spt 2000.