"INFORMATION WAR" FACTOR IN MODERN MILITARY CONFLICTS

Kaloyan A. Iliev

*Faculty of Artillery, Air Defense and Communication and Information Systems,
National Military University, Shumen, Bulgaria, kacho_78@abv.bg*

***ABSTRACT**: The coming war is one of the paradigms that are the subject of many futuristic analyzes and forecasts. Predicting its features and character is a difficult but not impossible process. Each of the modern armies is trying to change in order to adapt to future challenges. To this end, military specialists and experts are constantly working hard to develop new concepts, doctrines, and concrete programs.*

***KEY WORDS**: Information War, Doctrines, Future challenges, Information Impact.*

„ИНФОРМАЦИОННАТА ВОЙНА“ - ФАКТОР В СЪВРЕМЕННИТЕ ВОЕННИ КОНФЛИКТИ

Калоян А. Илиев

Въведение

"Този, който умее да води война, покорява чуждата армия без да се сражава, превзема чуждите крепости без обсада и разрушава чуждата държава без да държи дълго войската си. Той запазва всичко и така си оспорва властта в Поднебесната.".
Сун Цзи

Бъдещата война е една от парадигмите, които са обект на много футуристични анализи и прогнози. Предсказването на нейните особености и характер е труден, но не невъзможен процес. Всяка от съвременните армии се старае да се променя така, че да се адаптира към бъдещите предизвикателства. За тази цел военните специалисти и експерти непрекъснато полагат огромни усилия в разработването на нови концепции, доктрини и конкретни програми.

Според военните специалисти войната търпи развитие в няколко епохи: праисторическа, антична, средновековна, ранно модерна, индустриална и модерна. По своята структура тя се подразделя на отделни кампании, операции, сражения, боеве и удари, провеждани на театъра на войната, на отделни оперативни направления и райони. Целта на всяко едно военно ръководство е приключване на военният конфликт във възможно най-кратки срокове, посредством провеждане на успешни действия от различен мащаб и с различна цел. През последните години особена популярност доби концепцията за информационна война. Тя се основава на твърдението че информацията и информационните технологии са стратегически ресурс, от жизненоважно значение за националната сигурност и за военните действия.

Информацията играе съществена роля във военното (а и всяко друго) противоборство от най-древни времена. Счита се обаче, че именно в края на XX-ти век информацията и знанието придобиха решаващо значение за военния успех.

Информационната война ще измести на заден план конвенционалните форми за водене на бойни действия. Информацията е била и ще бъде все по важна за воденето на войната на всички нива, тя се очертава като четвъртия фактор, заедно с трите традиционни оперативни фактора - пространство, време и сили. Най-новите възгледи за бъдещата война бяха отразени в последното издание на „Наставлението за провеждане на операции на сухопътните сили на САЩ“. В него се предвижда, че бъдещите бойни действия ще се развиват в три макросфери: физическа, информационна и морална.

Информационното въздействие е преднамерено или непреднамерено въздействие на върху човека, чрез предаване на информация (сигнали, съобщения, сведения, образи). Основният обект на информационно въздействие е съзнанието на човека, групата, или общественото съзнание. С помощта на такова въздействие може преднамерено или непреднамерено да се изкриви картината на обективната реалност. Целите на това изкривяване могат да бъдат различни: от модификация на поведението на личността и управление на колективното (обществено) съзнание, до патологично нарушаване на психическите и физиологични процеси в човека.

Съвременните възгледи за въоръжена борба в информационната макросфера предвиждат те да протекат под формата на стратегически информационни операции. Основната им цел е да се постигне информационно превъзходство над противника на театъра на бойните действие и да се осигури ефективно командване и управление в хаоса на сраженията. Едновременно информационните операции ще пречат на противника да направи същото, създавайки "възпиращо триене" в когнитивните цикли на неговата командно-управленска система. Днес концепцията за информационната война заема важно място в общата парадигма за бъдещата война. Тя е важен инструмент за гарантиране на националната сигурност на всички нива - тактическо, оперативно и стратегическо.

Възгледите за въоръжена борба в моралната макросфера са тясно свързани с информационната и с основание се интерпретират като един от видовете информационна война. Тя се реализира като последователност от психологически операции, както в подготвителния период, така и по време на размяната на огневите удари. Целта е да се постигне морално превъзходство над противника, като се ослабят неговите съпротивителни сили и воля за победа. В последните години се забелязва трайно намаляване на желанието да се използват традиционни методи за война, като използването на физическо насилие, особено ако информационните операциите са успешни. Известно е, че днес може да не се обявява официално война срещу нечии врагове, като се използва военна сила и стандартните методи на огнево поразяване. По-ефективно е да се води скрита информационна война, която е значително по-лесно приложима. Независимо от това дали си даваме сметка или не, психологическите информационни операции са всекидневна реалност. Победите и загубите в тях формират бъдещия световен ред и етиката на човешкото общество. Медийните форми на психологически информационни операции бяха широко прилагани от всички участници във войната в Косово от 1999 г. (Операция Съюзна сила), войната в Афганистан през 2001-2002 г. (операция "Трайна свобода") и от войната срещу Ирак през 2003 г. Поведението на медиите през тази войни показа, че те са станали част от инструментариума на военните стратези и се третират като важно средство за въоръжена борба. С огромната си тиражност, глобален обхват и неограничена памет съвременните глобални информационни системи превръщат медийните психологически операции в стратегическо оръжие за въздействие върху човешката цивилизация.

В публикуваната литература се формулират и обсъждат 7 вида на тази офанзивно-агресивна форма на Информационната война:

- Радиоелектронна;
- Психологическа;
- Културна;
- Хакерска;
- Икономическа;
- Кибер-война;
- Война на Гибсън.

Радиоелектронната борба е една от най-добре осветените в литературата у нас. Основния обект на атаката са системите ISR и C4I на противника. Класифицирани по обектна ориентация, основните методи за борба са:

- Антирадиолокационни;
- Антикомуникационни;
- Криптографски.

Психологическата война е основана на използването на глобалното разпространение на информация по масмедиите (радио, телевизия). Тази форма води до обработка на общественото мнение в глобален мащаб, в необходимата посока. Ефектът от такава операция е твърде значим. Въздействието обикновено е пряко срещу личния състав и срещу командването. Наличието на полеви мултимедийни компютърни студия и компютърни TV - приемници, осигурява предаването на информация в реално време с цел - въздействие на противника. Въздействието върху командването е главно насочено към дезориентация, объркване и емоционално разстройване. Съществена е възможността за внасяне на невярна информация по отношение на намеренията на атакуващата страна и нейните възможности. Добавянето на агентурите информационни канали в тази посока дава значителен резултат.

Културната война се реализира в такива битово-обществени явления като Бързата закуска, Холивуд, Мадона, рисуваните филми, сините джинси и т. н., които според редица автори са проява на нова форма на културна агресия. Експанзията на чужда култура формира ново информационно-културно пространство, подменящо коренните национални традиции и ценности, възпитаващо космополитизъм и мултинационалност. Културната война е и политика. Емигрантската вълна, изтичането на мозъци на запад, както и импортът на културни продукти от запад са основните проявления на тази тиха и невидима война.

Хакерската война като правило се формулира като атаки срещу компютърните мрежи на противника. Използват се известни "дупки" в хардуера или софтуера. Въздействията могат да бъдат: тотална парализа на мрежите, междинни спирания, въвеждане на случайни грешки в потока данни, кражба на информация, кражба на услуги, незаконен мониторинг на системата и събиране на разузнавателна информация, въвеждане на фалшив трафик на съобщения, модификация на наличните данни с цел - въвеждане в заблуждение. Обикновено се атакуват цивилни цели (компютърни мрежи). Военните такива са обект на "командно -управленска война". Естествено физическото разделяне на двата вида системи прави военните по-защитени и недостъпни. И тук могат да се разграничат дефанзивна и офанзивна стратегии. Атаките срещу компютърните мрежи могат да са на физическо, синтактично и семантично равнища. Проблемите за военните системи на физическо равнище са сравнително малко. Със синтактичните атаки днес се постига най-значителен ефект. Семантичните атаки са предмет на отделен вид - "Кибер-война". Дефанзивните форми на хакерска война са насочени към защитата на компютърните мрежи и са дискутируеми като отделни форми, поради мощните защити на комерсиалния софтуер. В някои случаи се предлага атаката като най-добра форма на защита. Офанзивните форми са абсолютно нови форми и са в процес на синтезиране, анализиране и експериментиране. Основен въпрос е тяхната реална приложимост. Интернет, Електронната поща, предаването на данни и мултимедийните реализации, интегрирани в кабелно-разпределителните среди, осигуряват великолепни условия за подобни форми на разрушаване на инфраструктурите на стопанския живот на противника.

Затягането на многослойните системи за хардуерна и софтуерна защита се противопоставя на изобретяването на нови хитроумни способи за тяхното преодоляване. Особено важно е да се осигури защитата на компютърните системи за управление на енергийни, противопожарни, медицински, транспортни, телефонни, охранителни и др. подобни технологични компютърни системи. Отделен раздел на този вид война е компютърната вирусология, която е добре известна у нас. Терористичният характерна този вид война е особено опасен. Естествено редица природни бедствия носят по-разрушителен характер, но този вид въздействие е по-трудно доказуем и оценим като упражнения.

Икономическата информационна война се третира като информационна блокада и информационен империализъм. Блокадата по своята същност е прекъсване на потока от информация, както сега се прекъсва потока от стоки и материални ресурси. На практика се отнема печалбата от международния информационен обмен. Инфо-блокадата включва и физическата блокада на информационните носители. Прекъсва се достъпа в реално време до спътници, ретранслатори, GPS & GSM сателитни системи, картографски информационни системи и др. За подобна блокада е необходимо да се притежава контролът върху световните информационни ресурси във вид на глобално присъствие като международен оператор. Това за сега е възможно само в рамките на консорциум на най-развитите в икономическо отношение страни. С по-нататъшното разпространение на информационните връзки и тяхното интензифициране в глобален мащаб, все по-трудно ще става информационното блокиране на отделни държави или групи лица. Информационният империализъм може да се третира като разновидност на икономическият империализъм, поради тясната зависимост между стопанската дейност и информационното и осигуряване. Като цяло, тази форма може да се разглежда като продължение на търговската конкуренция с други средства. Аналогията с културната война е очевидна.

"Кибер-войната" включва: информационен тероризъм, семантични атаки и стимулационни войни. Информационния тероризъм е атака на персоналните файлове, на отделната личност. Те са в личния компютър и в обществени и квази-обществени бази данни, в областите на обучението, здравеопазването, административните услуги, търговията и финансовото обслужване и др. Семантични атаки водят до резултат, който е в вид на работеща система, даваща периодични груби грешки в информационно-обработващия процес. Смисловата същност на сензорната информация, или съдържанието на базите данни се подменя, с което се обезсмисля процесът на вземане на решения. Този вид атаки ще е особено болезнен в гражданските системи за обработка на информация (здравеопазване, финанси, материално-техническо снабдяване и др.). Стимулационната война е чисто и безболезнено провеждане на война на базата на добро симулиране, подобряващо непрестанно своята достоверност. Резултатът е една точна оценка на изходът от конфликта. Така противникът се убеждава, че ще загуби и взема съответните решения.

Ефектът от притежаването на по-добри бойни средства, в съчетание с тяхното умело използване, може да се демонстрира чрез симулации, без да се употребяват върху жива сила. Основният ефект от тази форма на борба е възможността операторът да моделира и прогнозира състоянието на бойното поле. Така по методът на "пробите и грешките" може да се оптимизира поведението в конфликта. На практика по-добрата техника за симулация, ще даде по-добро поведение. В този смисъл стимулационната война е война за по-пълни, по-достоверни, по-точни и по-надеждни модели на военните системи. По добрата система ще даде по-добри планове за действие. Автоматичното управление на сензорната мрежа и оръжията, на базата на вградените модели, прави войната по-между им стимулационно -моделна.

Войната на Гибсон (Виртуална реалност) е основно - борба на виртуалните реалности. Тя е тясно обвързана с бъдещето на Интернет и глобалните информационни мрежи, в частта "мултимедийни симулации". Войната на Гибсон третира аудио-визуалното присъствие на "воинът" в информационното и кибернетичното пространства. Стимулационните и Гибсон- войните са очевидни бъдещи модели, които ще се напълнят с практическо съдържание, при по нататъшното технологично развитие на глобалните информационни системи. Очевидно, този момент не е далече.

Като всички останали, войната с информационно-базирани оръжия предполага превъзходство, победа и загуба. Едновременно тя е нож с две остриета. Тази форма на информационна война е в неразривна връзка с останалите форми на противоборство, като отбранителните форми са явно по-ефективни и ясни.

Съгласно теорията на древния китайски владетел и пълководец Сун-Цзи, опознаването на културата на противника е основна задача на воюващият. Ролята на информацията в този процес е огромна. Неприятелските бази данни, алгоритми за обработка, комуникационни топологии, сензорни възможности и използвани знания за моделиране и управление са от първостепенна важност.

Разпространението на глобалните информационни инфраструктури и внедряването на висшите информационни технологии във военното дело радикално промениха съотношението между огневата мощ и информационното осигуряване, което продължава да се променя с високи темпове, в полза на информационното осигуряване. Тази тенденция наложи да се преразгледат фундаменталните приоритети в структурата на въоръжените сили, тяхната екипировка, въпросите на командването и управлението, бойната подготовка и персоналният тренинг. На практика, превръщайки се в основен способ за радикално решаване на възникналите кризи и конфликти, информационните операции се превърнаха в една от основните стратегически заплахи за националната сигурност. В края на столетието Интернет, сателитните телевизионни системи, оптичните кабелно-разпределителни мрежи и мултимедийните технологии са монопол на малка част от човечеството, която предопределя тяхното развитие и начин на използване. Публичността на информационните канали и носители дава възможност за достъп до тях на всеки. Но този достъп днес е поставен под контрол и е собственост на малка група държави, корпорации и частни лица, които получават едно ново стратегическо превъзходство.

Днес оперативният командир може надеждно и когато е необходимо, непрекъснато да комуникира с все по-разсредоточени сили в зоната на операцията. Информацията може да бъде предадена и получена в световен мащаб, в рамките не само дадена зона, но също и на стотици и хиляди километри извън границите, в които са разположени приятелските и вражеските сили. Новините за военните действия се излъчва в реално или в почти реално време. Глобалната информационна среда вече има дълбоко въздействие върху геополитиката, икономиката, военните дейности като цяло и операциите. Колкото повече една страна използва информация, толкова е по-уязвима нейната икономика и общество от нарушаване или дори парализа от действията на враждебни правителства или групи, проявяващи прикрита или явна враждебност. В информационната война географското местоположение и разстояние оказват съществено влияние върху използването на интернет.

Логично възниква въпросът за мястото на въоръжените сили в борбата за господство в световното информационно пространство. Създаването на възможности за тотален контрол и управление на информационните канали на въоръжените сили, позволява на реализиралия го:

- да концентрира и подчини човешките знания и култура на военната практика, като ги използва в реално време в боя;
- да създаде нова концепция за организацията и управлението на въоръжените сили, базираща се на превъзходство (доминиране) със знания на бойното поле.

Новите информационни техники и технологии позволяват на оперативните командири и техните екипи да имат много по-подробна и точна информация отколкото са имали в миналото за всички аспекти на физическо пространство. Това е критичен елемент в оценката на оперативният командир за ситуацията при планиране и провеждане на кампании или операции.

На практика който успее да усвои новите информационни техники и технологии в процеса на управление на войските, ще си осигури максимално превъзходство над този, който е закъснял да направи това.

Информацията играе съществена роля в командването и управлението на силите. Веднъж започнали военните действия, командира трябва да бъде в състояние да коригира плановете си с цел намаляване на уязвимостта. Началото на това, което се нарича обща оперативна картина за командирите на всички нива на командване се превръща в реалност. Подбираната или непълна информация се заменя със стандартизирани комплекти съобщение, които предлагат по-малко възможности за объркване или двусмислие.

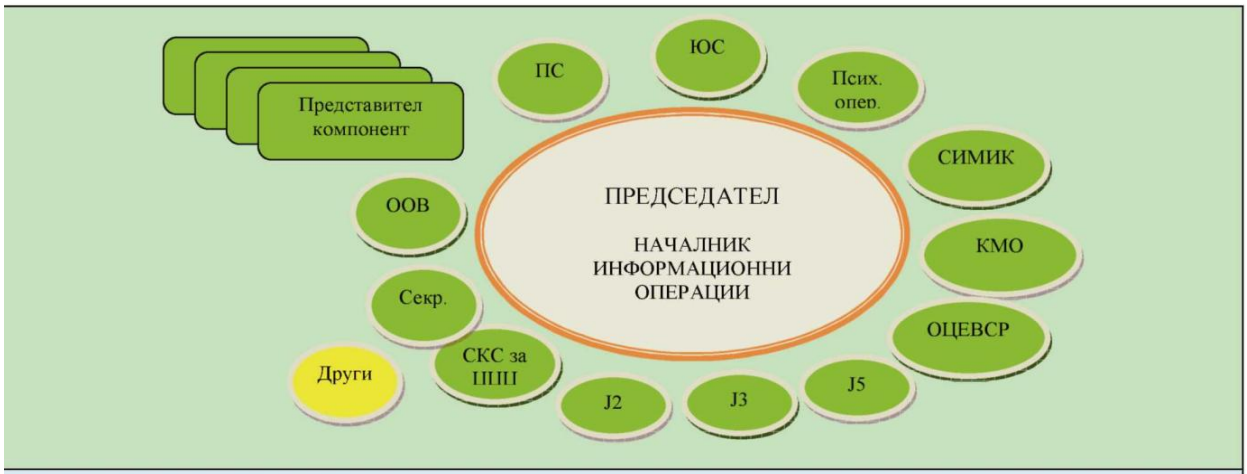
Погледнато през призмата на Въоръжените сили провеждането на информационни операции, представляват един елемент от глобалното информационно противоборство. Ето защо информационната политика и стратегия трябва да са постоянно действащи, а не да се формират за конкретна операция. Този пропуск може да се избегне чрез приемане на постоянно действащи документи в тази област, които трябва да са в съответствие с действащите съюзнически документи. Само тогава ще можем да говорим за равностойно участие на въоръжените ни сили в информационни операции в многонационална среда. В НАТО е приета директива за стратегическите ко-

муникации ACO Directive (AD) 95-2, ACO Strategic communications, 18 April 2012 и политика за информационните операции Military decision on MC 0422/4, NATO Military policy on information operations, 20 July 2012, които са двата основни регламентиращи документа на съюза в областта на информационните операции, прилагането на които е предпоставка за съвместимост между националните и съюзните способности в тази област, както и възможност за постигане на информационно превъзходство при провеждането на съвместните операции.

Информационните операции са интегрираща функция, насочена към информационната среда, а не толкова към способностите. Информационните цели са степен от планираното координиране и съгласуване на всички военни възможности, инструменти и техники, засягащи информацията или информационните системи. Употребата на сила може да допринесе за постигане на желания ефект в информационната среда. Всички планове и дейности следва да бъдат координирани и синхронизирани, с разрешени противоречия, за да не се правят компромиси с една дейност, което да доведе до отхвърляне или намаляване на желания ефект от друга. В многонационалните съвместни сили тази координация е отговорност на органите провеждащи информационните операции и се синхронизира в **Координационния съвет за информационни операции**. Той е подчинени на съвместния координационен съвет и е неразделна част от него, като в следствие на неговата дейност се изготвя анекс по информационните операции, като приложение към съвместната координационна заповед. Вариант на състава на координационния съвет за информационни операции е посочен в фигура № 1.

Фигура № 1

Координационен съвет за информационни операции (вариант)



Псих.опер.-психологически операции.
СКС за ЦЦЦ-представител от съвместен координационен съвет за таргетинг
ЮС-юридически съветник.
ПС-политически съветник.
КМО-компютърно мрежови операции.
Секр.-секретар.
J2, 3, 5 - представители от отдели.
ООВ - офицер по обществени въпроси.
ОЦЕВСР - оперативен център за електронна война и сигнално разузнаване.

- *ядро*
- *изисквани*

Съвместният координационния съвет за информационни операции допринася за реализирането на таргетинг процеса чрез номиниране на цели, които могат да повлияят чрез своите действия на провеждането на информационните операции. Съвместния координационния съвет за информационни операции съветва за последяващо появяване на нежелани ефекти в информационната среда и координира военните информационни дейности с цел избягване на нежелани ефекти.

Друг аспект на информацията е сътрудничество с медиите. Военните лидери на всички нива трябва да са наясно, че в ерата на информацията всички военни събития и действия се представят чрез медиите и това може значително да повлияе на общественото мнение, както и на ангажираността на силите.

Информацията включва не само познания и разузнавателни сведения, но и разнообразна информация от страна на медиите, която засягат морала, дисциплината, единството и мотивацията за борба. Информацията също оказва влияние върху морала на населението а оттам и на волята на страната да се бори. Това пряко или косвено влияе върху политическото ръководство и оперативния командир. По този начин информацията е едно от най-важните съображения при вземането на стратегически и оперативни решения.

Информацията все по-често засяга всичките три традиционни оперативни фактора. Нейният ефект върху фактора на пространството нараства, особено в невоенни аспекти на ситуацията. Това вече има някои съществени последици върху използването на военни сили за изпълнение на оперативните и стратегическите цели, което я определя като основен оперативен фактор. Стойността на информацията не трябва да се подценява, но също така не трябва и да се преувеличава. Информацията трябва правилно да се разглежда като помощ за оперативният командир и неговия щаб. Самата сложност и количеството на информацията се увеличават и ще имат решаващо влияние върху бъдещите резултати на кампаниите или операциите.

Заключение

Резултатите от направеното изследване позволяват да се направят следните **изводи**:

1. Войните в края на изминалия век нагледно показаха, че превъзходството ще е на страната на онези военни организации, които имат по-голяма информационна мощ, т.е. по-добра обработка на информация в инфраструктурните си подсистеми;

2. Бъдещата война ще е изцяло организационно явление, в което всяка от страните ще използва своята държавна мощ за унищожаване на противника. В началото на XXI век ще сме свидетели на невиждан синергизъм в концентрацията на тази мощ, постигнат чрез тотално използване на информационните технологии;

3. Като отчитаме тенденцията на насищане на съвременните информационни инфраструктури с качествено нови средства и технологии и особено автоматизацията на управлението на страните в мирно и военно време, можем да направим извода, че опасността от несанкциониран достъп в тях и провеждане на информационни операции нараства. Това е причината за предприемане на решителни мерки от редица държави по изграждане на информационна отбрана и защита на населението от информационна агресия и опазване на националните интереси в информационното пространство.

4. Характерът на бъдещите информационни конфликти, в повечето случаи ще се формулира като "не военни операции". Малко ще са нациите, които ще имат възможността да водят стратегическа информационна война във всичките и форми. По-скоро тези войни ще са локални, краткотрайни и едностранни по форма и вид.

5. Информационната война е концепция за постигане на решителните (крайни) военни и политическите цели чрез използване на нови нетрадиционни средства и форми на въоръжена борба за въздействие върху обществените информационни инфраструктури на противника с цел - нарушаване (или разрушаване) на организационния интегритет и командно-управленската свързаност на обществото и постигане по този начин на решителните (крайните) военни и политически цели на военната кампания.

6. Анализът на фигура №1 показва, че съществува определена зависимост между информационните операции и съвместния таргетинг процес.

Литература:

1. Желев, Ж. Отговорности при планирането на информационните операции. *Сборник научни трудове – част I*, 2014, стр. 78-85, ISSN 1313-7433.
2. Доктрина на Въоръжените сили на Република България, С., 2011, НП-3,
3. Доктрина за провеждане на операциите, С., 2012.
4. Национална отбранителна стратегия, С., 2011.

5. Стратегия за национална сигурност, С., 2011.
6. Alexandrov, B. Petrov, V. ISIS/ISIL into the “Internet” – Political and Military Weapon. *Годишник на Национален военен университет* „Васил Левски“. Велико Търново: НВУ „Васил Левски“, 2017, стр. 274-283. ISSN 1312-6148.
7. AJP-3.1, Allied joint doctrine, for Information operations, 2009.