ТИМЪТИ ТОМАС ЗА КЛЮЧОВИТЕ ЕЛЕМЕНТИ НА РУСКИЯ ПОДХОД КЪМ ИНФОРМАЦИОННАТА ВОЙНА

Тодор ТАГАРЕВ

В първата част на материала за американския изследовател Тимъти Томас,[1] публикуван в бр. 1 на списание "Информация и сигурност,"[2] представихме някои основни изводи за различията между руските и американските схващания за информационната война, пояснение за терминологичните различия и анализ на причините за уникалните руски възгледи за значението, ролята и мястото на информационните операции в съвременния свят.[3]

В миналото определяният като руски подход към изучаването на военните операции се отличаваше с няколко ключови елемента, сред които са вижданията за принципите на войната (тринадесет руски срещу девет в американските военни доктрини), характера на въоръжения конфликт, коефициентите на ефективност на ядрените оръжия, оценката на военния потенциал на възможен противник, корелацията на силите на две противостоящи страни, концепциите за контрол на въоръженията като възпиране и паритет. Сегашното изучаване на военните операции отразява много от тези елементи, но от гледна точка на информационните операции. Това е очевидно от изложените в предшестващата статия концепции за информационна сигурност и информационни операции. И макар че няма пряк паралел, възможно е да се наблюдава процес на приспособяване на военното мислене, довело до появата на термини от вида: разработване на информационно-психологически операции; изследване на интерфейса компютър-оператор; влияние на информационните операции върху понятия от контрола на въоръженията, например паритет; детайлна оценка на информационния потенциал на дадена страна; влияние на информационните операции върху военното изкуство, в частност върху

разбирането за начален период на войната; използването на компютърни вируси като оръжие; разработването на неврокомпютри и развитие на инфосфера; способността да се използват космически и информационно базирани средства за откриване и унищожаване на противниковите сили със скорост, точност и скритост.

В своя прецизен анализ на тези въпроси Тимъти Томас очертава десет ключови характеристики на руския подход към информационната война, представени детайлно в настоящата статия. [4]

Търсене на обективни закономерности и принципи на информационната война

Първият ключов елемент, уникален за руския подход към информационната война, е свързан с така наречените от теоретиците естествени закони и принципи, асоциирани с информационната война. Според проф. С.А. Комов, разкриването на обективните закони и принципи на информационната война е от първостепенна важност за развитието на научна теория на информационната война. Адмиралът от запаса Пирюмов твърди, че вече е направил това, и отбелязва, че общите универсални закони и принципи на въоръжената борба остават валидни и приложими за информационната борба. Но информационната борба има свои собствени специфични и вътрешно присъщи закони и принципи. Пирюмов изброява следните обективни закономерности на информационната борба:

1. Постоянно нарастваща роля на информационните бойни действия (информационната война) в изпълнението на поставените задачи в бойните операции на войските (силите). Определя се първично от нарасналата информатизация на въоръжените сили и вторично от увеличаването на силите и средствата, предназначени за тази информатизация. Необходимо е да се отбележи, че появата на нови средства и методи за информационна война не води до отхвърляне на традиционните средства, методи и форми на въоръжена борба, но оказва въздействие върху методите за решаване на бойни задачи с традиционни средства и променя възможностите на традиционните средства и ефективността на бойното използване на войските (силите).

2. Информационната война днес се води както във военно, така и в мирно време. Във втория случай средствата за информационна война се прилагат за снижаване на информационните ресурси на противника преди началото на бойните действия. Трябва да се отбележи, че

провеждането и последствията на информационната война не винаги са известни на страната, срещу която тя е насочена.

3. Постоянно нарастващото влияние на информатизацията на всички нива и сфери на правителствената и военната системи за управление осигурява в известна степен основа за идентифициране на информационната война като независима форма на въоръжена борба. Причината е, че повечето развити страни днес притежават мощен информационен потенциал, който при определени условия може да бъде концентриран и приложен за постигането на техните собствени политически цели. Привлекателността на този подход към решаването на външни политически конфликти се определя от два фактора - наблюдаваната в момента тенденция да се избягва използването на въоръжена сила в международни конфликти и отсъствието на международни законови норми, които да регулират методите за провеждане на информационна война.

Според Пирюмов организацията и провеждането на операциите (бойните действия) в информационната война следват няколко основни принципа:

- Подчиняване на целите и задачите на информационната война на задачите на войските в бойните действия; организация на информационните операции в съответствие с намерението и плана на операцията (бойните действия);
- Изпреварващо решаване на задачите на информационната война по отношение на бойните задачи на войските в бойните действия;
- Многоцелево използване на силите и средствата за информационна война в подготовката и провеждането на бойните действия, както и рационално комбиниране на мерките за информационна война с действията на войските за унищожаване на противника;
- Постоянно и скрито провеждане на информационна война през цялата операция (бойните действия);
- Принципа на противодействащата система, според който силите и средствата, назначени за провеждане на информационна война, трябва да бъдат обединени във функционална система, която по никой начин да не отстъпва на противниковата система за командване и управление.

Разбира се, изложените закони и принципи не са вечни. Напротив, те постоянно се уточняват в процеса на развитие на съдържанието, формите и методите за водене на информационна война.

Цели и методи на информационната война

Вторият ключов елемент отразява руските виждания за основните цели и методи за прилагане на концепциите за информационна война. Тимъти Томас счита, че това е основната разлика между руските и американските възгледи за информационна война, произтичаща най-вече от диференциацията на мирновременни и военновременни задачи.

Според Пирюмов *в мирно време* информационната война се води тайно със средствата на разузнаването, политиката и психологическото въздействие. Провежданите мероприятия са насочени срещу въоръжените сили, цивилното население и системата за управление на производството, изследванията и културата. Всяка страна се стреми да подкопае информационната сигурност на личността, обществото и държавата на противниковата страна, като в същото време пази собствената си информационна сигурност. Основна роля тук играят правителствените институции за пропаганда, външното разузнаване и контраразузнаването, както и институциите за защита на информация. Най-важен е фактът, че постоянно нарастваща роля играят специално програмирани хардуерни и софтуерни способи, насочени срещу информационните средства от техническата система на противника. А това е именно вирусната война.

Във военно време информационните операции са по-открити. Те действат като система, поддържаща традиционните форми и методи на война. Те поддържат също така информационните и разузнавателните мероприятия и секретността на основната дейност на собствените и съюзнически войски в подготовката и провеждането на операции. Те допринасят за постигане на изненада (особено в период на заплаха, какъвто е началния период на войната) и могат драстично да намалят информационните възможности на силите и да понижат бойния им потенциал, като в същото време защитят собствените сили (вероятно за тази цел ще е необходимо да се разработят системи и оборудване, устойчиви на противниково въздействие). Основният начин е да се извади от строя противниковата система за управление на войските и оръжията, като се защитят аналогичните руски системи.

В руското разбиране основни методи и средства за въздействие върху военните информационни системи са:

- Физическо разрушаване или действия за предотвратяване на функционирането като пленяване на личния състав или други действия на диверсионни групи и специални подразделения, огневи удари срещу системата, действия на разузнавателни групи, въздействие върху техническото състояние на системата;

- Електронно противодействие срещу указани командни пунктове и електронни системи;
- Използване на специално програмирани хардуерни и софтуерни способи срещу информационните елементи на автоматизираните системи за управление или за изненадващо разрушаване или блокиране на информационните системи на потенциално опасни държави в началото на бойните действия;
- Промяна на информацията, използвана от противника при оценяването на оперативно-стратегическата обстановка или в процеса на вземане на решение (чрез психологически операции или манипулиращи въздействия);
- Психологическо въздействие на информационните операции върху лидерите или военнослужещите от системата за управление на войските.

Главните компоненти на информационната война са:

- Специални операции за нарушаване на функционирането противниковото командване и управление;
- Радиоелектронни атаки;
- Информационна блокада, например чрез използване на радиоелектронна блокада;
- Системни действия на силите и средствата с функционално предназначение в информационната война.

Според Пирюмов информационната война се води на три нива: държавно, научно-технологично и на ниво военни системи и технологии. На държавно ниво целта на информационната война е да се снижи информационния потенциал на възможни противници, като в същото време се поддържа информационната сигурност на държавата. На научно и технологично ниво се цели технологично превъзходство за осигуряване на равновесие или превъзходство във военна мощ на основата на модерни информационни и технологични постижения. На ниво военни системи и технологии целта е да се провеждат действия срещу източници на информационна заплаха за да се елиминира, подави или намали тяхната ефективност. При това се взимат мерки за защита на елементите на собствената система за командване и управление.

Обществено въздействие

Трета, според Т. Томас първична, разлика между руския и западните подходи, е фокусът, в който руските изследователи поставят въздействието на информацията върху гражданите. Този “информационно-психо-

логически" аспект на информационната война не е дотолкова доминиращ в САЩ, където основните интереси са насочени към електронната война, механизмите за защита и нападение, цифровизацията във въоръжените сили и информационното доминиране. Т. Томас счита, че американското общество поне засега е относително стабилно и разглежда възможното чуждо въздействие върху американското мислене и психика за минимизирано. Но руското безпокойство е разбираемо, тъй като с разпадането на Съветския съюз обществото е загубило своя споряващ механизъм - комунистическата идеология. Според много руски социолози и учени единствено контрол върху "информационно-психологическия" аспект може да гарантира духовна стабилност на страната, така необходима за успешно продължение на реформите и опровергаване на слухове и дезинформация.

В подкрепа на това свое становище Т. Томас привежда като пример изявлението на кандидата за руски президент и лидер на Комунистическата партия Генадий Зюганов, който счита себе си за жертва на информационно-психологическо мероприятие в предизборната кампания на Елцин през юни и юли 1996 год., като подчертава важността на информацията за руското общество със следните думи:

> Налага се да се махнат кавичките от концепцията за "четвъртата власт" и законово да се признае, че държавните електронни мас-медии са автономен - информационен - орган на властта заедно със законодателната, изпълнителната и съдебната власт.

Ударението, поставено от Зюганов, съответства на традиционното значение, отдавано от руските военни на морално-психологическите фактори, които разглеждат морално-психологическия като един от тринадесетте принципа на войната.

Човекът във фокуса на подхода към информационната война

Четвъртият елемент, тясно свързан с информационно-психологическия, е сериозният опит на руските учени да впрегнат енергията, генерирана от човека. Те вярват, че така наречения "проблем на сигурността на компютърния оператор" е мултидисциплинарен и изисква интеграция на различни области от знанието - физика, биология, психология, кибернетика, философия и религия. От тази гледна точка човекът се разглежда като отворена система, комуникираща със средата посредством материални, енергийни и информационни потоци. Тогава е възможно чрез излъчване (електромагнитно, акустично и др.) да се повлия на човека и да

се предизвикат промени в неговото психофизиологично състояние. Не само енергийни източници, но и "пакетираната" по подходящ начин информация може самостоятелно да въздейства върху жизненоважни процеси в човека. Според Томас силно повлияни от тази теория са автори в областта на информационните операции като Виктор Солнцев и Владимир Пирюмов.

Солнцев например вярва, че хората възприемат света като различни форми на информационни потоци и всеки човек обработва тези потоци по различен начин. Според тези учени, определени форми на радиационни (енергийно)-информационни полета могат да предизвикат болест, разстройство на жлезите и системите на организма, промяна на поведението, подтискане на мисловните процеси, манипулиране на съзнанието и разрушаване на самосъзнанието. Докладвани са дори смъртни случаи, предизвикани от човеко-машинния интерфейс:

> Воронеж, 13 август 1994 год. За по-малко от 20 минути потребител на персонален компютър загубил съзнание. Приятелят му - програмист - казал, че имал странни усещания, като че ли … имал главоболие и странен шум в ушите. Било почти невъзможно да го спре - като че ли бил под хипноза. За щастие успял да изключи компютъра си. Малко по-късно приятелят му починал без да дойде в съзнание. Поставената диагноза - мозъчен кръвоизлив.
>
> Смъртта била причинена от компютърен вирус с името "666". Експерти установили, че вирусът предизвиква поява на компютърния монитор на така наречения 25-ти кадър със специална цветова комбинация, която довежда оператора до хипнотичен транс. Всеки 25-ти кадър картината се променя. Подсъзнателното възприемане на новия образ води до сърдечна аритмия. Кръвното налягане внезапно се покачва, а после рязко спада. Кръвоносните съдове на мозъка не издържат на тези импулси. В последствие са регистрирани близо 50 случая на внезапна смърт.[5]

До сега руснаците не са обсъждали открито собствения опит в използването на компютърно генерирани "упойващи" образи, но в редица случай се позовават на използваните от САЩ холографски изображения в Сомалия и в операцията "Пустинна буря." Освен това тази област е сред приоритетните за руския Комитет за наука и технологии. Томас приема като многозначително поставянето в списъка на Комитета на провежданите изследвания върху системи за разпознаване и синтез говор, текст и

изображения, както и на системи за изкуствен интелект и виртуална реалност. Някои руски учени вярват, че посредством човеко-машинния интерфейс може да се влияе върху технически обекти, съзнанието на отделен човек и дори върху груповото съзнание на дадена общност от хора.

Геостратегическа значимост

Руските изследователи разглеждат развитието на информационните операции като явление, което има не само тактическо и оперативно, но и *геостратегическо значение*. Така например, превъзходството в информационните технологии може да осигури начини за пряко въздействие върху ядрените кодове или командната процедура по изстрелването на балистични ракети. Традиционни мерки за стратегическо равновесие като брой и мегатони на носители и заряди ще загубят смисъла си когато информационните технологии дадат възможност за изваждане от строя на системите за изстрелване и управление на ядрените носители или снижат значително тяхната надеждност.

Руските специалисти вярват, че развитието на системите за информационна война, включително на системите за разузнаване, води до нарушаване на съществуващите норми за ядрен и конвенционален паритет, които са базирани главно на брой и технически характеристики. Разузнаването, командването и управлението, ранното предупреждение, комуникациите, електронната война, "специалните софтуерни ефекти" и дезинформацията допринасят за превъзходството на бойното поле по качествено нов начин и нарушават традиционната сравнимост на войските и силите. Освен това, те могат да бъдат използвани като скрита форма на военно-политически натиск.[6] В този смисъл Русия разглежда информационните операции като ключов геостратегически елемент с възможности за нарушаване на статуквото. Така например, те могат да имат катастрофално въздействие в редица области: информационен удар срещу стратегически команден пункт, срещу националната електрическа мрежа или срещу системата за управление на ядрена електроцентрала с последващо неконтролируемо развитие на ядрените процеси. Нещо повече, удари от такъв характер могат да бъдат нанасяни както във военно време, така и скрито в мирно време.

Информационен потенциал

Руските специалисти изчисляват информационния потенциал на дадена страна като степен на нейната информационно-базирана военна мощ.[7] Компонентите на информационния потенциал включват две основни

области - *информационни ресурси* и *информационни способи*. Пирюмов определя информационните ресурси като информация, която се събира и съхранява в процеса на научните изследвания, практическата дейност на човека и дейността на специални организации и средства за събиране, обработване и представяне на информация, записана на магнитен носител или по друг начин, осигуряващ доставянето до потребителя в необходимото време и място за решаването на научни, производствени и управленски задачи. Заслужава внимание и категорията *информационен потенциал на оръжие*, определян като степен на неговото "информатизиране", т.е. степента до която вътрешните компоненти на оръжието зависят от информационни или компютърни функции за постигане на максимална ефективност.

Въздействие върху военното изкуство

По мнението на руски специалисти информационните операции оказват огромно въздействие върху изучаването на оперативното изкуство. Те разглеждат тези операции както като самостоятелен тип конфликт, така и като операции, които повишават неопределеността в началния период на войната (неизвестна е мирновременната подготовка на потенциалния противник за промяна на ефективността на оръжията или за въздействие върху стратегическата оценка за ситуацията в началото на войната), или като операции за повишаване темпото на боя, непрекъснати действия за заслепяване на противника чрез разрушаване на неговите способности за провеждане на информационни операции и за постигане на информационно доминиране.

Ако под въздействието на информатизацията и компютъризацията се променя формата на бойните действия, то ще последват и промени във военното изкуство. Пирюмов например вярва, че въздействието върху военното изкуство се проявява по три начина. Първо, бързото развитие на средствата за комуникация, появата на различни автоматизирани системи за управление и увеличения брой бойни средства днес позволяват координиране на бойните действия на хетерогенни войски и сили и тяхното огнево взаимодействие *без да е необходима пространствена концентрация*. Второ, компютъризацията и използването на оборудване и системи за дълбоко разузнаване позволяват да се повиши точността на разрушаване на противникови средства и системи. По този начин концепцията за "борбата на вторите ешелони" създава възможности за нанасяне на високоточни селективни удари срещу подхождащите резерви на противника, неговите тилови ресурси, и т.н. И накрая, операциите вече

няма да се провеждат циклично с интензивни действия и затишия. Те ще имат непрекъснат характер, като особено важно е да се унищожава противника веднага след неговото откриване. Това означава, че военните действия ще се развиват в посока "*откриване-унищожаване*" и неизбежно ще се стигне до концепцията "*разузнаване-удар-(електронно) подавяне*". *Решаващо превъзходство ще постигне страната с управление в реално време* и това ще доведе до ново ниво на компютъризация на въоръжените сили. Победата в борбата за ефира ще означава и победа в боя.

По мнението на Цимбал воденето на информационна война оказва влияние и върху трите нива на военното изкуства - стратегическо, оперативно и тактическо. Той отбелязва, че целта в мирно време ще бъде да се натрупва информация за противника, като в същото време се разработват и тестват собствени оръжия за информационна война. Непосредствено преди и по време на военните действия системите за информационна война ще се използват преди всичко срещу системата за управление на войските на противника, както и срещу други информационни системи, които получават, съхраняват и обработват информация с военно значение. Освен това е възможно информационната операция да се провежда независимо преди началото на традиционните бойни действия.

Може би най-важните цели, идентифицирани при изучаване на военното изкуство, са бойните системи, които откриват и веднага след това унищожават даден обект, а именно разузнавателно - ударните комплекси. За да се изпълни това е необходимо да се развият възможности за точна оценка на резултатите от удара в реално време и за противодействие на опити за маскировка и заблуда. Руски учен предлага следната математическа формула за описание на процесите, водещи от откриване към поразяване на обект:

> *възможност за поразяване = откритост на обекта по отношение на спътници или други разузнавателни средства* X *точност на ударните средства и скорост на техните компоненти*

Всички средства за разузнаване, добиване, управление, повишаване на точността и т.н. са взаимно обвързани и се контролират от инфосферата (вж. десетия ключов елемент), разбирана като съвкупност от програми за обработка, съхраняване и създаване на данни. Спътникът определя местоположението на обекта, високоточното оръжие използва данните, изпратени от спътника, а скоростта и точността на оръжието зависят от неговите информационни компоненти.

Развитието и структурирането на въоръжените сили по начин, съвместим с казаното по-горе, е приоритет и една от областите на единомислие на руските и западните изследователи. Дори бегъл преглед на руски военни публикации ясно подчертава важността, придавана на определянето на положението на противника с последващо въздействие с огневи средства. Както отбелязва Сергей Григориев

> Повишаването на огневите възможности на войските, появата на високоточни оръжия и разработването на различни видове управляеми ракети обективно водят до повишаване на ролята на разузнавателните системи и системите за командване и управление. При условие, че вероятността за точно попадение в целта с първия изстрел или залп се приближава до единица, скоростта на реакция придобива извънредна важност. Главни цели на разузнаването на бойното поле са противниковата артилерия и бронетанкови средства.

В резултат развитието на способности за откриване на цели понастоящем е от първостепенна важност за руските военни. Само в периода 1994 - 1996 год. на страниците на "Военна мисъл" се появиха не по-малко от седем статии по въпроса за ефективно целево въздействие, тоест как най-ефективно да се получи необходимата информация и да се унищожат противниковите цели. Изчерпателната дискусия отрази и такива аспекти като: зоналното или точковото целево въздействие е по-ефективно; как то може да се интегрира в критериите за успешни съвместни бойни действия; и редица други. Например в една от статиите се отбелязва, че продуктивното целево въздействие "зависи главно от това *колко бързо информационните потоци от разузнавателните органи се трансформират в командно-управленски импулс към средствата за въздействие върху целите*." Това е случаен процес, но е възможно да се оценят неговите статистически свойства.

Поставянето на ударението върху процеса на откриване, опознаване и определяне на местоположението на целите съвпада с промените във военното изкуство, прогнозирани от Пирюмов.

Генерал-полковник Н.М. Димидюк, Главнокомандващ Ракетни войски и артилерия на Сухопътни войски, обобщи дискусията за ефективното целево въздействие във "Военна мисъл". Той призова за по-тясна интеграция на средствата като отбеляза, че "в сегашните условия ефективното целево въздействие не може да бъде отделено от електронното подавяне на противниковите системи и мрежи за командване и управление, информация и разузнаване." В резултат ефективното целево въздействие се издига до нивото на "решаващ фактор, определящ курса и изхода на

бойните действия, а в много случай, и на войната като цяло …" Силите и средствата за ефективно целево въздействие ще се използват "да нарушат функционирането на противниковите системи за управление на войски и оръжия в самото начало на операцията, да причинят решителни загуби на главните сили на противника и тиловото му осигуряване, да завоюват и удържат огнево превъзходство …" чрез тяхното координирано и масирано използване с постигане на изненада. Тази координация ще изисква като основна задача да се постави

> координирането на плана за ефективно целево въздействие с целите, замисъла и плана на операцията, което може да се осигури само ако планирането се извършва от органа за управление на оперативния съвместен щаб чрез Група за планиране и координиране на ефективното целево въздействие … Това ще измести центъра на тежестта при планиране на ефективното целево въздействие към оперативното ниво …

В заключение Димидюк отбелязва:

> Резултатите от дискусията показват, че при оценката на ефективното целево въздействие е подходящо да се използва един показател с ясна физическа интерпретация, който лесно може да се интегрира в използваните критерии при планиране на операциите - очакване на скоростта за изваждане от строя на противниковите войски. Този показател трябва обективно да отразява ударните, разузнавателните, маневрените и други възможности на разглежданите войски (сили), които характеризират тяхната поразяваща мощ в атака и оперативна устойчивост в отбрана. Накрая трябва да признаем, че все още не е направено достатъчно за извеждане на необходимите зависимости между силите на страните в операции от различен тип и мащаб, когато бойните им възможности се изразяват чрез техния боен потенциал.
>
> … По отношение на хомогенни цели (брой цели от един и същи тип) ефективното целево въздействие се определя чрез частта от индивидуални цели, върху които се оказва въздействие, докато по отношение на цели от различен вид (хетерогенни цели), то се определя от техния състав (комбинация), като при това може да има няколко такива комбинации. Предполага се, че ако върху поне една цел от тази комбинация не е въздействано ефективно, тя запазва бойната си способност и е в състояние да изпълнява функциите си.

Компютърни технологии

Компютърните изследвания доведоха до някои неочаквани резултати, уникални за руския опит. Т. Томас определя като един от тези резултати невронния компютър, от който се очаква да замени чипа Pentium по скорост и ефективност. Като технологии в информационната област с приоритет на федерално ниво правителствения Комитет за наука и технологии определя:

- Мулти процесорни компютри с паралелна структура
- Компютърни системи на базата на невронни мрежи, транспютри и оптически компютри
- Системи за разпознаване и синтез на говор, текст и изображения
- Изкуствен интелект и системи за виртуална реалност
- Информационни и телекомуникационни системи
- Системи за математическо моделиране
- Микросистемни технологии и микросензори
- Свръхголеми интегрални схеми и наноелектроника
- Оптична и акустична електроника
- Криоелектронни производствени технологии
- Лазерни технологии
- Високоточни и мехатронни технологии
- Роботизирани системи и микромашини
- Електронно-йонно-плазмени технологии
- Интелектуални системи за автоматизирано проектиране и управление

Особен интерес в този списък представляват неврокомпютрите. Т. Томас цитира доклад, според който разработваните в Русия неврокомпютри са 1000 пъти по-бързи от традиционните. Те намират военно приложение в създаването на модерни високоточни оръжия, военно оборудване, оптични уреди за откриване на ракети, както и в програми за антибалистична защита и технологии с двойно назначение. Те се използват и във финансовите пазари за прогнозиране на валутни курсове, акции и други активи, като според руски доклади осигуряват 90 % точност.

Системен анализ

Признавайки нарастващата важност на системния подход, руските учени фокусираха вниманието си върху взаимодействието на бойни системи вместо върху опростения модел на двустранно противодействие. Според

Томас този подход се отличава от американския по своя диалектичен характер и включва оценяване на бойните системи една спрямо друга вместо изолирано. На базата на тази логика войната се разглежда като взаимодействие между конфронтирани военни системи. Идеята е достигнала до използваните модели в Генералщабната академия, където вече не играят по старите модели на "червени срещу сини." Вместо това се моделира противодействието на високотехнологични системи. Аналитици отбелязват и особената важност на системната интеграция:

> … разузнавателно-информационно-управленските компоненти осигуряват *системен интегритет*. Затова интеграцията също се разглежда като обект на информационната конфронтация; нейната дезорганизация, неутрализация или разрушение води до нарушаване целостта на системата и до загуба на нейните потенциални възможности.

В рамките на военната системология информацията се разглежда като "храна," която дава живот на всички елементи на системата отгоре до долу. В частност това се отнася до системите за разузнаване, командване и управление, поддръжка и поразяване. В съответствие с този възглед информационната война като система включва три компонента: информационна поддръжка на функционирането на собствените информационни системи; информационно противодействие срещу функционирането на бойните системи на противника; информационна защита или отбрана на собствените бойни системи от информационното противодействие на възможен противник.

Накратко, страната, която не може да управлява в реално време огъня по войските на противника е обречена не само в мащабен конфликт, но и в някои конфликти с ниска интензивност. Ударението се поставя върху способността да се добива и обработва информация чрез пространствено разпределени системи за откриване, идентификация и определяне на положението на цели. Според Григориев

> бързо расте броя на информационните източници за тактическите системи за управление на войските. Все по-широко се използват разузнавателни дистанционно пилотируеми летателни апарати. Радиолокационното откриване и авиационните пунктове за командване и управление се усъвършенстват. Всичко това води до нарастваща взаимна обвързаност и взаимозависимост на оръжията с въздушно и земно базиране. Ефирът все по-ясно се отличава като 'четвърто измерение' на бойното пространството. В него се

заглушават радиолокационни станции и комуникационно оборудване, откриват се и се унищожават източници на излъчване, заслепяват се електрооптични системи за наблюдение.

Инфосфера

Един от най-важните фактори от техническа гледна точка е инфосферата, определяна от Кукашкин и Ефимов като "съвкупността от общи и специализирани програми за създаване, обработка и съхраняване на компютъризирани данни, която *ще се превърне в един от най-вероятните обекти на военна конфронтация*." В частност, руските учени са обезпокоени от въздействието на вражески действия, насочени срещу инфосферата. Предполага се, че за такива цели могат бъдат използвани два вида "оръжия" - "алгоритмични" и "софтуерни" бомби. Алгоритмичните бомби изменят част от даден алгоритъм, в резултат на което се ограничава способността на програмното осигуряване да функционира по необходимия начин. Софтуерните бомби вмъкват нежелан алгоритъм, който ограничава изпълнението на функциите на програмното осигуряване или го насочва към извършване на неоторизирани и непредвидени изчисления. Този последен ключов фактор играе главна роля и в американския подход към информационната война.

Идеята е описана за пръв път в статия на капитан Владимиров от 1991 год. Той отбелязва, че

> В продадената на Ирак френска противовъздушна система са били инсталирани така наречените "логически бомби," което предотврати използването й срещу многонационалните сили по време на военните операции в Персийския залив. Американска ракета се отклони от курса и бе взривена по команда от земята, тъй като нейната компютърна програма индикира '1' вместо '7' … ефективността на компютрите зависи от качеството на софтуера. Дефекти под формата на неправилно написани части от програми често водят до пълен срив на системите … Саботирани грешки значително влошават проблема за качеството и надеждността на софтуера.

И тъй като именно софтуерни програми движат много от системите, не е изненада, че Русия е разработила вируси за въздействие върху тях. Руският аналитик Александър Поздняков изброява четири типа компютърни вируси, макар че не става ясно дали се позовава на техни руски или американски варианти. Руснаци твърдят също така, че са разработили вирус "стелт." Този вирус не може да бъде открит с обичайните методи. Руски учени очаква към двехилядната година да се сблъскат и с

“дистанционни вирусни оръжия” - компютърни вируси, вмъквани чрез радиоканали или лазерни комуникационни линии директно в компютрите. Това се разглежда от тях като пряка заплаха за системите за управление на части и подразделения, като например части от ракетните войски със стратегическо назначение. Последната разглеждана заплаха се състои в използването на “микровълнови оръжия,” генериращи електромагнитни импулси срещу електронните компоненти на руските средства за защита от информационна война с космическо, въздушно, земно и морско базиране. Според някои източници Русия изследва възможността за разработване и прилагане на аналогични средства.

По мнението на руски специалисти, инфосферата може да се превърне в цел на вражески намерения в мирно и военно време. Такива атаки са най-опасни, когато са насочени към системи за откриване, идентификация и определяне положението на цели и към системата за управление на страната.

Заключение

Десетте ключови елемента, очертани от Т. Томас, характеризират терминологичните и концептуални особености на руския подход към проблемите на информационната война. Но наистина ли тези елементи са различни от западния подход?

Очевидно е, че относително лесно могат да се идентифицират цели на информационните операции в дадена страна. Системите за електронна война, възлите на системата за управление на войските, спътниците и самолетите АУАКС днес се открояват така, както бронетанковите формирования преди 50 години. Съществените различия са в концептуалното разбиране за информационните операции от културна, идеологическа, историческа, научна и философска гледна точка. Различни логически призми могат да ни доведат до тотално различаващи се заключения относно намеренията, назначението, фаталността и нарушаването на суверенитета при използването на информационни операции. Тази логика може да доведе и до съвсем нови творчески методи за атакуване на цели.

Руският подход отразява диалектическата логика и формиралите го исторически процеси, както и усилията за адаптация към една нова среда. Така например в близкото минало в Русия доминираше контролът над информацията. Много хора дори нямаха достъп до копирни машини. Днес Русия се бори с пълзяща “информационна анархия,” от която по мнението на руските граждани обществото е преситено. Гражданите просто не знаят на какво да вярват когато четат вестници или гледат телевизия. Проблемът

е също толкова труден и за военните. Разбирането за заплахите е развивано в течение на много години. И макар че има поводи и причини за сътрудничество със Запада, руските военни се включват много предпазливо. Много от тях все още оценяват края на Студената война като успешна информационна операция на Запада, разрушила не само Съветския съюз, но и комунизма - обединяващата идеология на страната. И сега си задават въпроса дали Западът няма да подхване друго подобно амбициозно начинание за да разшири контрола си върху Русия.

Според Т. Томас главното притеснение на САЩ е, че в опита си да настигне Запада в областта на информационните операции Русия изглежда няма ясна представа къде може да се окаже в края на процеса. Този факт се отразява и върху начина, по който военните определят термини като ‘информационна война.‘ Определенията им са много по неясни, отворени за интерпретация и предизвикващи повече недоразумения, отколкото в миналото. Какво имат предвид руснаците, когато определят някое действие като “информационно-психологически” удар? Нещо по-важно, какви са допустимите съставляващи на такива действия? До какво ще доведат те - обвинение в нарушаване на международните закони или взаимно нанасяне на ядрени удари? Кои са областите на недоразумение, които биха довели до аналогичен отговор от страна на САЩ?

Ако искаме да избегнем информационна конфронтация или война в бъдеще ще са необходими още много усилия за преодоляване на терминологичните и концептуални проблеми, свързани с уникални и ограничени възгледи за информационните операции. Десетте изброени елемента конфигурират един уникален и определено различен подход към проблема. В продължаващото сътрудничество на САЩ и други страни с Русия всеки трябва да обръща по-голямо внимание на мисленето на другия в тази чувствителна област. Също както в миналото Русия и САЩ бяха загрижени за ядрените оръжия, сега те трябва да търсят способи за предотвратяване на конфликти и управление на кризи. Нещо повече, необходимо е да се направи сравнителен анализ на китайски, американски, руски, канадски, германски, британски и други възгледи, както за да разберем дълбочината на проблема, така и за да избегнем настоящи и бъдещи проблеми в областта на информационните операции.

---

[1] Информация за Timothy Thomas е публикувана в бр.1 на списание “*Информация и сигурност*” от 1998 год.

[2] Тодор Д. Тагарев, "Сравнителен анализ на руски и американски възгледи за информационната война в работите на Тимъти Томас," *Information & Security. An International Journal* 1, 1 (Summer 1998), 105-115.

[3] Детайлно разглеждане на терминологичния апарат е направено от автора в статията "Еволюция на понятието 'информационна война'," *Военен журнал* 105, 3 (1998), 80-86. Анализ на някои български схващания за информационната война е направен в доклада Velizar M. Chalamanov, "Information Warfare in Depth - A Personal View from Eastern Europe," *19th AFCEA Europe Symposium* (Brno, Czech Republic, 28-30 October 1998). Българските разбирания са отразени и в статията на генерал Михов, публикувана в предния брой на списанието.

[4] Настоящата статия е базирана на следните публикации на Timothy Thomas:

- "Dialectical versus Empirical Thinking: Key Elements in the Russian Approach to Information Warfare," *Slavic Military Studies* 11, 1 (March 1998), 40-62.
- "Russian View on Information Based Warfare", *Airpower Journal* 10 (Special edition, 1996), 25-35.
- "The Mind has No Firewall," *Parameters* 28, 1 (Spring 1998), 84-92.
- "Russia's Information Warfare Infrastructure," *European Security* (forthcoming).
- "'Intellectual' IW and the Tolstoy Factor: Russia's PSYWAR-IW Interface," *Military Review* (forthcoming).
- "The Russian PSYSOP and Information Operations Interface," *Special Warfare* (Winter 1997).

Част от тези публикации са достъпни и чрез Интернет на адрес

http://leav-www.army.mil/fmso/fmsopubs/fmsopubs.htm

[5] Този случай бе отразен и в българските медии. Томас се позовава на Victor I. Solntsev, "Information War and Some Aspects of Computer Operator's Defense," *InfoWarCon 5* (Washington D.C., 4-6 September 1996): 2-7.

[6] *Независимое военное обозрение*, 18 ноември 1995 год.

[7] Близко е определението за *информационна мощ*, предложено от Велизар Шаламанов и Тодор Тагарев в книгата *Информационни аспекти на сигурността* (София: Прокон, 1996).