Сравнителен анализ на руски и американски възгледи за информационната война в работите на Тимъти ТОМАС

Тодор ТАГАРЕВ

Информацията играе съществена роля във военното (а и във всяко друго) противоборство от най-древни времена. Счита се обаче, че именно в края на XX век информацията и знанието придобиха *решаващо* значение за военния успех. Анализите на подготовката и провеждането на бойните действия в Персийския залив през 1991 г., както и на съпровождащите ги политически, дипломатически и медийни изяви, убедително демонстрираха приносите на модерната технология за постигането на военна победа. Ентусиазмът, основан на огромните възможности на информационните и комуникационните технологии, доведе до появата на съвременния термин *информационна война*, а войната на коалицията на ООН срещу Ирак бе обявена за първата информационна война.

Водеща роля в развитието на концепцията за информационна война играят американските военни. Само две от причините за това са широкото внедряване на най-модерни информационни и комуникационни технологии и опита от войната в Персийския залив. Но дори американски изследователи отчитат взаимното влияние и проникване на идеи, концепции, стратегии и доктрини. Пример за това дава дискусията относно революцията във военното дело в американските военни среди. Признава се, че американските разработки са повлияни значително от руските (съветските) теории за военнотехническата революция и революцията във военното дело, зародили се през 70-те години.

В продължителни периоди без мащабно реално използване на въоръжените сили от особено значение е наличието на информация за тактически, оперативни и стратегически концепции на партньори и на потенциални противници. При отсъствието на конфронтация добиването на съответното

INFORMATION & SECURITY. An International Journal 1, 1 (Summer 1998), 105-115.

знание и изясняването на позициите на отделни страни е значително облекчено. Убедителен пример за това ни дава изследователската и публикационната дейност на о.з. подполковник от Сухопътните войски на САЩ Тимъти Томас.

Томас е световнопризнат експерт по проблемите на руските възгледи за информационната война. Неговите сравнителни анализи на руски и американски военни схващания за информационните операции са уникални. Нещо повече, на прага на третото хилядолетие те разкриват важни закономерности за бъдещи военни конфликти. Защото информационната война вече изживя "детската си възраст." Концепцията за информационна война постепенно намира своето място сред традиционните схващания за ролята на военния инструмент в гарантирането на националната сигурност, сред методите и формите на противоборство на стратегическо, оперативно и тактическо равнище, в пространствено-временните релации както на класическия тип конфликт, така и в подготовката и провеждането на операции, различни от война.

Не е трудно да се открият прилики между руския и американския подход към информационните операции. Специалисти от двете страни отделят голямо внимание на електронната борба и системите за управление на войски и сили и подчертават значението на компютрите и мениджмънта на информация в подготовката и провеждането на съвременни военни операции, в това число и използването на информация при провеждането на психологически операции.

Но детайлният анализ на руските възгледи в работите на Т. Томас показва, че руският подход към информационните операции се характеризира с някои особености, които го правят уникален и различен от западните подходи. Томас идентифицира три групи причини за тази уникалност:

Социално-икономически причини. Руските държава, икономика и общество са в преходен период, довел до институционално и философско неравновесие. Според мнението на много изтъкнати учени и официални лица руското масово съзнание е уязвимо по отношение на манипулации чрез ловки рекламни кампании и експлоатиране чрез обещания за икономически и социален просперитет. В резултат в подхода си към информационните заплахи руските специалисти поставят ударение на така наречените информационно-психологически процеси и законодателните подходи за гарантиране на индивидуалната и обществената информационна сигурност.

Военнотеоретични причини. Руската военна мисъл е резултат на своеобразно развитие. Географски съображение, различни военни заплахи, икономически реалности, породени от различната идеологическа основа, и ударението на изучаването на военното дело като наука рефлектират върху мисловния процес

на военните. В резултат руското изучаване на въздействието на информационните оръжия върху военното изкуство се различава от западното по начина на разглеждане и оценяване на съответните операции.

Финансови, технологични и инфраструктурни ограничения. Руският подход е уникален и в резултат на специфичните финансови, технологични и инфраструктурни ограничения върху развитието на информационния потенциал. Инфраструктурата просто не може да поеме огромните изисквания на технологичното усъвършенстване в Информационната ера. Телефонната система, която в повечето градове не може да поеме обикновените позвънявания, трудно ще бъде адаптирана за значително по-високите изисквания на компютърните комуникации. От гледна точка на технологиите години ще минат до появата на оптични кабели в някои райони. Едва неотдавна руски компютърни компании започнаха производство на изцяло руска елементна база. Жестоките бюджетни ограничения спъват усилията за бърза промяна. В резултат руските учени отделят повече време за развитие на *теорията* на информационните операции в сравнение със западните си колеги, чиито усилия са насочени главно към практиката. На Русия ще са необходими няколко години да настигне Запада в технологичната област. Но изостаналостта може да се превърне и в предимство, когато други плащат за грешките в развитието на технологии от първо поколение (ако приемем, че има някакво ниво, на което може да бъде достигнато относително равновесие).

Руските специалисти приемат тази изостаналост като факт и се опитват да я преодолеят. Макар внедряването на информационни технологии да продължава вече 15 години, производството на модерни системи започна едва преди около пет години. При необходими около 450 хиляди компютъра в момента са внедрени само 25 хиляди, което прави 18 % "информационен коефициент на интелигентност." С този темп за достигане на коефициент 90 % ще са необходими 50-60 години. След като започна самостоятелно производство на компютри, Русия вероятно ще достигне тази бройка много по-скоро, стига бюджетът да позволи. Но ще бъде много трудно военният "информационен коефициент на интелигентност" да надвиши чувствително този на обществото.

Освен изброените по-горе причини важно е да се напомни, че за разлика от стотиците западни автори много малко руски експерти пишат за информационните операции в открити източници. Няма официално списание или документ на Министерството на отбраната, който да очертава руската концепция за информационни операции. Затова Т. Томас прави своя сравнителен анализ на основата на публикувани виждания на малък брой военни и офицери от запаса. За щастие голяма част от тях са не само експерти в областта, но и преподават по проблемите на информационните операции в

руските военни академии и институти.

В свои публикации през последните две години[1] Т. Томас определя и анализира детайлно десетте ключови елемента на руския подход към информационната война. Те ще бъдат представени в следващия брой на списанието. В този брой даваме кратко описание на руското виждане за понятията информационна сигурност и информационна война, които служат като основа на детайлното обсъждане. Сами по себе си тези определения са уникални, тъй като се основават на руския опит и диалектическа мисъл.

Определения за информационна сигурност

Руската концепция за национална сигурност, както и няколко закона определят информационната сигурност като национален интерес на Русия. През 1995 г. в там бе направен първият опит да се разработи Закон за информационната сигурност. Аналогичен документ в САЩ не съществува. В областта на отбраната тази уникална и широкообхватна оценка очертава няколко критични области - състоянието на информационната сигурност в Русия, възприеманите заплахи срещу нея, методите за гарантиране на информационната сигурност на държавата, организационната структура и принципите на действие на системата за информационната сигурност. В нея се изброяват следните *критични области*:

- Информационните източници на Министерството на отбраната, Генералния щаб, главните щабове на компонентите на въоръжените сили и научноизследователските звена; информация и факти /данни за подготовката и провеждането на оперативни и стратегически планове, разполагането на войски и мобилизацията, тактико-техническите характеристики на оборудването;
- Информационните ресурси на военнопромишления комплекс, както и за промишления потенциал и количеството налични суровини и материали; информация за основните насоки на разработките на оборудване за въоръжените сили;
- Системата за командване и управление на страната, личния състав и оръжейните системи, както и информационната им поддръжка;
- Морално-политическото състояние на въоръжените сили;
- Информационната инфраструктура (контролни точки и връзки, релейни точки, тропосферни и спътникови комуникации), включително и комуникациите с други министерства.

[1] В края на статията е приложен списък публикации, използвани при подготовката й.

Източници на външна заплаха:

- Всички видове разузнавателна дейност;
- Информационно-техническа дейност като електронна война и методи за проникване в компютри;
- Психологически операции на възможни противници както чрез специални дейности, така и чрез средствата за масови комуникации;
- Дейности на чуждестранни политически и икономически структури, които са насочени срещу интересите на Русия в сферата на отбраната.

Вътрешни източници на заплаха:

- Нарушаване на установените комуникации и информационни средства в щабовете и учрежденията на Министерството на отбраната;
- Преднамерени и непреднамерени грешки на персонала на информационната система със специална значимост;
- Информационно-пропагандна дейност на организации и личности, насочени срещу интересите на правителството, които водят до снижаване на престижа и бойната подготовка на въоръжените сили.

Работният проект отбелязва още, че тези заплахи са особено значими при влошена военнополитическа ситуация. Проектът раздели основните методи за повишаване на информационната сигурност в сферата на отбраната в три области: концептуална, техническа и организационна.

На основата на концептуалните методи се структурират целите при гарантиране на информационната сигурност на отбраната, например цели, произтичащи от практически задачи, правилно оценяване на информационните заплахи и техните източници. Методите от втората област служат за усъвършенстване на средствата за защита на информационните източници от несанкциониран достъп чрез разработване на защитени системи за командване и управление и повишаване на надеждността на компютърните ресурси. На основата на организационните методи се формира оптимална структура и състав на функционалните органи на системата за информационна сигурност в сферата на отбраната и се координира тяхното взаимодействие, усъвършенстват се методите за стратегическата и оперативна дезинформация, разузнаване и електронна война и се развиват методи и средства за активно противодействие на информационно-пропагандни и психологически операции на възможен противник.

Доколкото е известно, този проект все още не е приет като закон. Съществуват обаче и други закони (част от които във фаза на разработване) и законови актове, свързани с информационните операции.

Определение за информационна война[1]

Към момента няма официално руско военно определение за информационна война, одобрено от Министерството на отбраната, Съвета за сигурност или Съвета по отбраната. В изказвания и статии се дават няколко неофициални определения. Във всички случаи те се характеризират със стремежа да не се копира американското разбиране на термина. Според руския аналитик В.И. Цимбал "няма смисъл просто да се копират концепции за информационна война. В концепцията за информационна война на Министерството на отбраната трябва да бъдат интегрирани конституционните изисквания на Руската федерация, нейните основни закони, спецификата на сегашното икономическо състояние и задачите пред нашите Въоръжени сили." В допълнение Цимбал посочва, че в Руската федерация органите за държавна сигурност отговарят за информационната война в широкото разбиране на термина. Частично потвърждение на този факт е получено наскоро, когато Федералната комисия за правителствени комуникации и информация поиска Думата да й позволи да контролира Интернет в Русия. Комисията, която наследи бившето осмо главно управление и 16-ти директорат на КГБ, твърди, че ЦРУ създава информационни оръжия и бойни компютърни вируси, което налага поемането на контролни функции от нейна страна.

За разлика от американските определения във всички известни досега руски определения се забелязва една обща тема - информационната война се води в мирно и военно време. В неговото мирновременно значение терминът се отнася до информационната сигурност на обществото и държавния апарат в психологически, научен, културен и производствен аспект. Военновременното значение на термина се отнася до постигането на превъзходство в осигуряването на информационна защита и системи за подавяне, включително в командване и управление, електронна война и разузнаване.

Според Т. Томас може би най-авторитетният руски специалист, дал определение на информационната война към момента, е адмиралът от запаса Владимир Пирюмов. Той е бивш преподавател по радиоелектронна война, а в момента е съветник по научните въпроси на руския президент. Адмирал Пирюмов определя информационната война по следния начин:

Информационната война е нова форма на борба между две или повече страни, която се състои от целенасочено използване на специални средства и методи за въздействие върху информационните ресурси на противника, както и на защита на собствените информационни ресурси за постигане на определени цели. Под *информационен ресурс* се разбира информацията, събрана и съхранена в развитието на науката, практическата дейност на човека и действието на

специализирани организации и средства за събиране, обработване и представяне на информация, съхранена в магнитна или друга форма, осигуряваща доставянето до нейните потребители в необходимото време и пространство за решаване на научни, производствени или управленски задачи.

Неговото определение може да се тълкува в смисъл, че информационната война е дейност, която може да се извършва както в мирно, така и във военно време. Конкретно за военни сценарии Пирюмов предлага определение за информационна война в операции за завоюване на информационно предимство:

> Информационната война в операциите (бойните действия) е съвкупност от всички съгласувани мероприятия и действия на войски, провеждани в съответствие с отделен план за завоюване и поддържане на информационно предимство над противника по време на подготовката или провеждането на операциите (бойните действия). Наличието на *информационно предимство* предполага, че компонентите на системата за управление на собствените войски и оръжия са информирани в по-голяма степен отколкото тези на противника, притежават по-пълна, детайлна, точна и навременна информация от противника и условията и възможностите на собствената система за командване и управление позволява използването на това предимство в бойните действия на войските (силите).

Т. Томас отдава значение и на други руски определения на термина информационна война. В.И. Цимбал - цивилен аналитик в Министерството на отбраната - предлага две определения за информационна война:

> В широк смисъл информационната война е една от разновидностите на "студената война" и включва мерки за противоборство между две страни, прилагани най-вече в мирно време по отношение не само и не толкова към въоръжените сили, колкото към общественото съзнание, държавно-административната система, системата за управление на промишлеността, управлението на науката, културата и т.н. Именно в този смисъл обикновено се разбира информационната сигурност на личността, обществото и държавата.
>
> В тесен смисъл информационната война е една от разновидностите на военната дейност / операции/ действия (или непосредствената подготовка за тях) и има за цел постигането на тотално превъзходство над противника под формата на ефикасност, пълнота и надеждност на информацията при нейното получаване, обработка и използване, разработването на ефективни управленски решения и тяхното целенасочено прилагане за постигането на бойно превъзходство (победа) на тази основа. В този смисъл воденето на информационна война е част от отговорностите най-вече на министрите на отбраната на модерните държави.[2]

Последното определение, което разглежда Т. Томас, е дадено от полк. проф. С.А. Комов, кандидат на техническите науки, и е ограничено в рамките на военновременното използване на термина. Според него информационната война е

> …комплекса от информационна поддръжка, информационно противодействие и информационно-отбранителни мерки, прилагани по единен замисъл и план и насочени към добиването и удържането на информационно превъзходство над противника при започването и провеждането на военни действия/боеве. Трябва да се отбележи и взаимната обвързаност между информационната война и други видове оперативна/ бойна поддръжка и дейностите, които изпълват нейното съдържание (разузнаване, събиране на информация, комуникации, и др.).

В определението на Комов има четири ключови момента: първо, идентифицирането на мероприятия за получаване на информация за противника и условията на бойните действия (електронни, климатични, инженерни и др.), за събиране на информация за собствените и съюзническите войски и сили, за обработване и обмен на информация между пунктовете за управление и войските; второ, набелязване на мерки за блокиране на информационно-добиващите процеси на противника и за подаване на заблуждаваща информация на всички етапи; трето, разработване на собствени и съюзнически мероприятия за противодействие; и четвърто, постигане на информационно превъзходство над противника.

Какво показва сравнението на тези определения с американските определения за информационна война? Съгласно Директива S-3600.1 на Министерството на отбраната на САЩ, приета на 9 декември 1996 г., информационната война се определя като информационна операция, провеждана по време на криза или конфликт за постигане или поддържане на специфични цели спрямо конкретен противник или противници. Информационната операция се определя като действия за въздействие върху информацията и информационните системи на противника и защита на собствената информация и информационни системи.

Сравнявайки американските и руските определения, Томас открива както прилики, така и различия. И двете страни включват в определението концепцията за защита на собствената информация (в определението на Пирюмов - информационни ресурси), докато въздействат върху информацията на противника. В допълнение към информацията в тесен смисъл руските определения са по-широки и обхващат съображенията за информационната сигурност на обществото в мирно и военно време, докато американските определения се ограничават до времена на криза или конфликт.

Според Томас дори тази кратка дискусия демонстрира загриженост при обсъждане на информационните операции. Двете страни използват различен език и концептуални подходи в опитите си да определят основните термини. Американската страна например не определя "информационни ресурси," "информационно предимство" или (използвания по-късно) термин "информационен потенциал." Руснаците, от своя страна, се затрудняват в намирането на точен термин за концепцията за information warfare и използват няколко термина за нейното описание.

Но изясняването на терминологичните различия е от изключително значение. Макар информационните технологии да се разработват предимно за мирни цели, техният разрушителен потенциал е сравним с потенциала на ядрените технологии. Те могат да въздействат тихо и без предупреждение върху правителствени, обществени, бизнес и финансови институции, върху военните системи за командване, управление и комуникации. Всеки от тези атрибути на обществото може да бъде повлиян или изваден от строя без широко разпространено физическо разрушение, съпътстващо използването на ядрени и конвенционални оръжия. В ръцете на нерационални политици или криминални типове информационните технологии и техните възможности могат да бъдат също толкова опасни за държавния суверенитет и благосъстоянието на гражданите, както и въоръженото нападение, от което се опасявахме през Студената война.

Затова особено важно е да разберем какво другите мислят за информационната война, как възприемат и реагират на използването на термина, кои стъпки биха възприели за акт на информационна война. Стъпка в тази посока е запознаването ни с трудовете на Т. Томас.

ТИМЪТИ Л. ТОМАС (TIMOTHY L. THOMAS) работи като анализатор в Службата за чуждестранни военни изследвания (Foreign Military Studies Office) във Форт Ливънуърт, Канзас. Има звание подполковник от Сухопътни войски на САЩ, където служи до лятото на 1993 г. Получава степен бакалавър от военното училище в Уест Пойнт и магистър от Университета на Южна Калифорния. Служил е в Сухопътни войски като офицер за чуждестранни изследвания, като е специализирал по съветски / руски въпроси. По време на военната си служба е заемал длъжности на директор за съветски изследвания в Руския институт на американската армия (USARI) в Гармиш, Германия; инспектор по съветски тактически операции в рамките на Конференцията за сигурност и сътрудничество в Европа; заместник-началник щаб по разузнаването на бригада и ротен командир в 82-ра въздушно-преносима

дивизия. Т. Томас има обширна изследователска дейност и много публикации в областта на мироопазващите операции, информационната война, локалните войни и по военнополитически въпроси. Той е заместник-главен редактор на списание "*European Security*" и професор в Евроазиатския институт на Сухопътни войски на САЩ. Член е на две руски организации - Академията за международна информация и Академията по естествени науки.

Статии на Т. Томас са публикувани в руски издания и "*Чешка военна мисъл*." Няколко статии е изготвил в съавторство с руски офицери. Владее руски език. Тимъти Томас е член на редколегията на "*Международен журнал. Информация и сигурност.*"

Публикации на Т. Томас за последните две години:

Информационна война/ Информационни операции

"Russian View on Information Based Warfare", *Airpower Journal* 10 (Special edition, 1996), 25-35.

"Deterring Information Warfare: A New Strategic Challenge," *Parameters* 26, 4 (Winter 1996-97), 81-91.

"Dialectical versus Empirical Thinking: Key Elements in the Russian Approach to Information Warfare," *Slavic Military Studies* (forthcoming).

"Information Operations: How Russian Security Specialists Perceive the Threat," in *War in the Information Age* (Brasseys, 1997).

"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).

"Russian Information Operations: A Bibliography," *Law Enforcement and Low Intensity Conflict* (Summer 1997).

"The Age of the New Persuaders," *Military Review* 77, 3 (May-June 1997).

Lester W. Grau and Timothy L. Thomas, "A Russian View of Future War: Theory and Direction," *Slavic Military Studies* 9, 3 (September 1996), 501-518.

Информационни технологии

"Virtual Peacemaking: the Use of Information Technology in Conflict Prevention," *Parameters* (forthcoming).

"Information Technologies: Russian/U.S. Perspectives and Potential for Cooperation," (Chapter in a forthcoming book).

Локални войни и конфликти

"Russian Lessons Learned in Bosnia," *Military Review* 76, 5 (September-October 1996)

"Russian Air Operations in Chechnya," *Air Power Journal* 11, 4 (December 1997).

"The Battle for Grozny," *Slavic Military Studies* 10,1 (March 1997).

"Russian Lessons Learned in Bosnia," *Military Review* (December 1996).

---

[1] В тази част от своя анализ Т. Томас дава руски определения на термина Information Warfare. Поне част от дискутираните различия са на лингвистична основа и характеризират особености на използването на термина и на български език. В зависимост от контекста, английската дума "warfare" се превежда на български език като "война", "бойни действия", "противоборство" и др.

[2] Министър на отбраната на Русия е и най-висшия военен.