ИНФОРМАЦИОННИТЕ СПОСОБНОСТИ – ВАЖЕН ЕЛЕМЕНТ НА ИНТЕЛИГЕНТНАТА ОТБРАНА

С. Балабанов, Р. Илиев

Резюме: *В доклада се разглеждат информационните способности като важен елемент на интелигентната отбрана и свързаните с тях приоритетните проекти за повишаване на отбранителните способности на Българската армия. Представени са основни направления за повишаване на информационните способности, като са разгледани някои приритетни проекти за развитие на въоръжените сили на България. Разгледани са важни системи, осигуряващи съвременни информационни способности, като системите C4I, мрежовоцентрични, системи за съвместна работа и др.*

Ключови думи: *информационни способности, системи C4I, мрежовоцентрични операции, системи за съвместна работа, инвестиционни проекти*

УВОД

Информационните способности, като важен елемент на военните способности, определят способността на една държава да осигурява своя суверенност. Същността на ***отбранителните способности*** е в използването на изградения потенциал за постигане на мисиите и за решаване на задачите на отбраната при поддръжка на държавната политика за сигурност. Те интегрират концепции, доктрини, обучение, подготовка, организация, комплектуване, военни технологии, военна инфраструктура, бойна готовност и фокусирана логистика[4]. Изграждането на силите на Европейския съюз е насочено към достигане на необходимите способности за провеждане на съвременни високотехнологични операции и ефективно използване на наличните ресурси. В този аспект инициативата на НАТО „Интелигентна отбрана" за изграждане на отбранителни способности чрез многонационални и иновационни подходи, е "*възможност за нарастване на ефективността на усилията на страните-членки за изграждане на по-високо ниво на сигурност за сметка на по-малки разходи на ресурси чрез по-добро координиране и кооперирање на дейностите*", както отбелязва генералния секретар на НАТО Андерс Фог Расмусен на Мюнхенската конференция по сигурността.

Военните способности се определят на базата на дефинирани мисии и задачи на въоръжените сили, националните цели и амбиции и се изразяват в състава и структурите на въоръжените сили, личният им състав, инфраструктурата, въоръженията, техниката и логистиката. Военните способности на република България представляват единство от доктрини, организации, обучение, материални средства, лидерски умения, личен състав, инфраструктура и съвместимост, осигуряващи изпълнението на поставените задачи и постигане на желания ефект[2]. Изграждането на военните способности е непрекъснат процес на промяна на състоянието на военната мощ и е в пряка

зависимост от степента на развитие на икономиката, науката и технологиите, образователната система и културата на обществото. Като тенденция за развитието на военните способности все по-силно се очертава и четвъртото измерение на противоборството, наред с това по суша, въздух и море, а именно – в информационното пространство. Превъзходството в информационното пространство несъмнено изисква притежаването на ефикасни информационни способности за въздействие.

Информационните способности са наличие на потенциал за осигуряване на превъзходство, базиран на информацията като ресурс. Те се постигат чрез ефективно информационно осигуряване на всяка военна операция. Съвременните информационни операции са съществена част от военното дело. Нещо повече, те постепенно изместват центъра на тежестта към себе си и се налагат като доминиращи[9]. Във военното пространство, най-вече в средите на коалиционните партньори в НАТО, понятието *Мрежово-центрични военни действия* се наложи като обединение на методите и способите за използване на последните достижения на информационните технологии за осигуряване на информационни способности, необходими за постигане на информационно превъзходство и за превръщането му в бойна мощ.

Информацията винаги е била един от най-важните фактори във войната. Според Клаузевиц „*непълните знания за ситуацията ... могат да доведат военната акция до безизходно положение*". Очевидно е, че колкото повече една армия знае за себе си и за противника си, толкова по-силна ще бъде във войната. Това, което не е толкова очевидно е как да бъде използвана информацията и как знанията да бъдат манипулирани така, че да увеличат силата на армията многократно. Такава война е по същество информационна война и олицетворява сблъсъка на информация или знания във военните операции. Тя се определя, от една страна, като „действия за отхвърляне, използване, изопачаване, или унищожаване на противниковата информация и неговите функции", а от друга, „като защита на собствената информация и провеждане на наши собствени информационни операции"[6].

Информационната война е „нова доктрина, разработена за всеобхватното включване на информационно-обработващите процеси в структурата на въоръжената борба, при което информационните технологии се използват като:

- ✓ база за качествено изменение на средствата за въоръжена борба, като върху тях се прехвърлят рутинните интелектуални човешки функции;
- ✓ инструмент за постигане на стратегическо информационно превъзходство в когнитивния цикъл на управлението на въоръжените сили;
- ✓ нов специфичен вид поразяващи средства за водене на офанзивни бойни действия в информационната пространство, от нов вид въоръжени сили"[6].

Информационната операция, като основен елемент на информационната война, поддържа стратегическите цели чрез въздействие върху способността на противника да взема навременни и ефективни решения за използване на своите въоръжени сили. Важността на победата в информационното противоборство трябва да бъде водещ принцип във военните действия. Военните изследователи предвиждат, че ефективните информационни операции ще направят бойното поле ясно и разбираемо за нас и непрогледно и неразбираемо за противника. Един от командващите ВВС на САЩ във войната в Ирак също подчерта важността на информацията на стратегическо и оперативно ниво[15]: „*Във Войната в залива коалицията лиши Ирак от повечето от неговите способности да добива и обработва информация. В същото време, коалицията се справяше приемливо със собствените си информационни нужди. За бъдеще е ясно изискването за реконструиране на организациите така, че те да бъдат изградени за използване на модерно оборудване за информационни технологии*." Оттогава до сега в някои страни това стана реалност. C4I-системите вече се определят като „инструмент за тотално взаимодействие на всички равнища и на всички структури (включително и международни) за постигане на информационно превъзходство на бойното поле, който се основава на четири стълба: глобална мрежа, … базов команден комплекс, …тактическа информационна система за обмен на данни, …тактическият команден център" [7]. В САЩ дори се говори за въвеждане на система за следене и докладване на степента на готовност и работоспособност на компютърните мрежи, подобно на системата за бойна готовност на войските и силите.

РАЗВИТИЕ НА ИНФОРМАЦИОННИТЕ СПОСОБНОСТИ НА ВЪОРЪЖЕНИТЕ СИЛИ

Важността за развитие на информационните способности на Българската армия е видно от Националната отбранителна стратегия, приета през 2011 г., където информационните ресурси се разглеждат като основен елемент на ресурсите за отбрана. В нея се отбелязва, че „изпълнението на задачите, произтичащи от мисиите на въоръжените сили в голяма степен зависи от постигането на информационно превъзходство и ефективно взаимодействие" [3].

Информационните способности на Българската армия са свързани с „осигуряване на точна, навременна и защитена информация, гарантираща ефективното и прецизно управление и взаимодействие между органите за управление" [3]. Това се постига чрез създаване и поддържане на системи за наблюдение, разузнаване и автоматизиран обмен на информация, спомагащи за изграждането на пълна и опозната картина на общата обстановка и представляващи част от интегрирана комуникационно-информационна система от органи, комуникационно-информационни ресурси, процедури,

доктрини и документи за добиване, обмен, обработка, съхранение и защита на информацията, включително и от кибернетични атаки[3].

Според Националната отбранителна стратегия, развитието на информационните способности е свързано с изграждане и усъвършенстване на:

- ✓ Системите за наблюдение, разузнаване и ранно предупреждение както и пунктовете за събиране, обработка, анализ и обмен на информация на национално и съюзно ниво.
- ✓ Комуникационно-информационната система (КИС) на въоръжените сили (стацинарна и мобилна) като част от Единната интегрирана комуникационно-информационна система на страната.
- ✓ Мобилните тактически комуникации, осигуряващи оперативна съвместимост и управление на формированията в съвременна бойна среда.
- ✓ Способности за действие в мрежово-центрична информационна среда.
- ✓ Способности за превенция, откриване, защита и възстановяване след кибер-атаки.

Обобщените данни, получени в реално време от системите за наблюдение, разузнаване и ранно предупреждение, спомагат за повишване на информационните способности чрез предоставяне на пълна и опозната картина на въздушната, наземната и морската обстановка, която се предоставя на длъжностните лица в реално време.

Комуникационно-информационната система се поддържа от мирно време и осигурява управление на структурите и формированията при кризи от различен характер. Стационарната КИС обхваща стационарните комуникационно-информационни възли на защитените пунктове за управление на стратегическо и оперативно ниво, както и стационарната опорна комуникационна мрежа, като осигурява информационния обмен за управление на страната и въоръжените сили в мирно време и по време на война. Мобилната КИС, състояща се от мобилни модули, осигурява информационния обмен за управление на формированията от Българската армия и коалиционните сили на територията на страната и информационните потребностите на формированията от Българската армия, участващи в мисии и операции зад граница.

Способностите, осигурявани от мобилните тактически комуникации, се постигат с цифровизация на системата като цяло и с осигуряване на високоскоростен обмен на информация в реално време, необходими при модулно разгръщане и комуникационно осигуряване на бойни групи на голямо отдалечение от територията на страната.

Мрежово-центричната информационна среда осигурява способности за водене на военни действия базирани на бойна мощ, която може да бъде генерирана от ефективното свързване или мрежова работа на бойните

формирования[9]. Тя се характеризира чрез способността на географски разпръснати сили (състоящи се от единици или модулни формирования) да изградят високо ниво на споделена информираност между тях за бойната обстановка, която чрез само-синхронизация до осигури възможност за осъществяване на целите, поставени от командирите. Това се постига чрез трите ключови предимства на мрежово-центричните операции: информационен обмен между географски разпръснати сили; добра информираност на мрежово-центричните войски; ефективно свързване между единиците на бойното поле.

Способностите за превенция, откриване, защита и възстановяване след кибер-атаки е съществен елемент на информационните способности за осигуряване на сигурността. Те се постигат самостоятелно или съвместно със съюзниците чрез изграждане на единна интегрирана система за откриване, предупреждаване и реагиране на кибер-заплахи в компютърните мрежи и устройства, използвани за нуждите на отбраната[10].

Важен елемент за повишаване на информационните способности на Българската армия е развитие на системите за *командване, управление, комуникации, компютризация* (обработка на информацията) и *разузнаване* (откриване, наблюдение и разпознаване) - C4I. Във възприетите във Военната доктрина на република България принципни постановки за изграждане на боеспособни и ефективни въоръжени сили, развитието на C4I-системите е залегнало като приоритет и те имат водещо място. Сами по себе си, C4I-системите са компонент на система от системи *SoS*, която включва още ISR – системи за *откриване, наблюдение, разпознаване* и PGW – високоточни инструменти, технологии, техника и въоръжение[5]: *SoS = ISR + C4I + PGW.*

Системите C4I са свързан с решаването, както на вътрешните за страната въпроси, така и по отношение на оперативната съвместимост и приетите от страната цели за партньорство. Целите за изпълнение са заложени в плана за членство в НАТО.

Развитието на системите C4I в БА, включва следните основни принципи[12]:

- ✓ изграждане на единни информационни системи за мирно и военно време, с програмен принцип за реализация на проектите и задоволяване на всички оперативни изисквания;
- ✓ съвместимост между отделните подсистеми и с подбни национални системи, а където е необходимо и със системите C4I на НАТО, страните партньори и на съседите;
- ✓ мобилност на полевите системи, свързана с обработката и обмена на информация в хоризонтална и вертикална посока, като тя трябва да е непрекъсната, за да осигури бързо развръщане и действия на въоръжените сили;
- ✓ устойчивост, дефинирана като способност на системите C4I да поддържат всякакви операции, независимо от тяхната продължителност, при

осигуряване на надеждна защита на информацията на всички нива, според нейната степен на класификация.

C4I-системите трябва да осигуряват пълна, точна, навременна, поверителна, съвместима и ясна информация от отделният войник до всички щабове по командната верига и обратно (в съответствие с ISO 9241).

Поради важността на C4I-системите за осигуряване на информационни способности на въоръжените сили, в Инвестиционният план-програма на Министерството на отбраната до 2020 г. са включени три важни проекта[8]:

✓ Проект 7 „Придобиване на модул за комуникационно-информационна поддръжка на контингент", с което ще се осигурят в комуникационно и информационно отношение българските военни контингенти при участието им в операции и ще се създадат способности за действие в мрежова среда при осъществяване на националното управление.

✓ Проект 12 "Кибернетична защита", с който се осигуряват способности за повишаване на кибернетичната сигурност на съществуващи, изграждани и предстоящи за изграждане военни системи и мрежи, като се поддържа и развива център за наблюдение и анализ, и център за реагиране и възстановяване.

✓ Проект 13 „Развитие на автоматизирана информационна система на Министерството на отбраната, Българската армия, оперативните и тактически щабове", като се изгражда единна мрежова информационна среда за функциониране на системата за командване и управление на всички нива – стратегическо, оперативно и тактическо и подпомагане на дейността на структурите от Министерството на отбраната за успешно изпълнение на мисиите и задачите, чрез непрекъснат, бърз и надежден електронен обмен и достъп до общи информационни масиви.

В проектите за модернизация на C4I-системите в МО и БА се предвижда те да се интегрират в единна информационно-комуникационна среда, която да осигурява високо качество на услугите, оптимизирани финасови разходи за реализация и поддръжка, отвореност за потребителя ("user-friendly"). Това ще се постигне с широко прилагане на съвремени технологии и решения, като WEB, Cloud-computing, виртуализация, с използване на ефективни приложни системи, с реализация на високонадеждни сървърни архитектури и на подходящи средства за комуникация и защита на информацията.

За повишаване на информационните способности на въоръжените сили от съществено значение е създаването на съвместни информационни среди за общо ползване и споделяне на информацията. Компютърните системи за съвместна (групова) работа (Collaborative software, Groupware, Workgroup support systems) обединяват компютърен софтуер, проектиран да подпомага потребителите за съвместно решаване на задачи при постигане на общи цели. С развитието на технологиите тези информационни среди позволиха да се

обменят текстови съобщения (чат), глас и видео в реално време, а впоследствие и на специализирани приложения, като общи календари, информационни бюлетини, WEB-портали за съвместна работа и др.

Във военната област, прилагането на системи за групова работа, стартира в края на 80-те години. През 1990 г., правителството на САЩ започва истинско приложение на такива системи, като една от първите е системата „Компас", предназначена за съвместно оперативно моделиране, планиране и симулационна стратегия (Common Operational Modeling, Planning and Simulation Strategy – COMPASS)[11], предназначена за флота. В нея работят до 6 потребителя с изградени връзки помежду им, от тип „точка-точка". Моделът на работа се подобрява със създаването на т. нар. „виртуални работни станции за сътрудничество" (Collaborative Virtual Workstation – CVW)[14], които впоследствие прерастват в Информационно работно пространство (InfoWorkSpace – IWS).[13]

Прилагането на технологии и решения за съвместна работа в Министерството на отбраната и Българската армия, би повишило способностите чрез един по-оперативен начин на работа със спестяване на време, липса на необходимост от физическо събиране на участниците в едно помещение при брифинги и съвместни дискусии, ползване на единни информационни системи и ресурси и др. Освен това, голяма част от задачите, които се изпълняват, са свързани с общи, колаборативни процеси – съвместни обсъждания (брифинги) (*Real-Time Meetings*), подготовка и управление на съвместни документи за управление на войските (*Group Document Handling*), организиране на работни потоци по различни оперативни задачи (*Work Flow*), планиране и съставяне на графици на мероприятия (*Group calendaring and scheduling*), споделяне на знания, свързани с видовете осигурявания и управленски опит (*Knowledge Sharing*), подпомагане вземането на решения от командира, съгласно 5-степенния модел за оперативно планиране на НАТО (*специализирани приложения*) и др.

Една от първите информационни среди за съвместна работа, с прилагане на съвременни технологии за повишаване на информационните способности в сигурността и отбраната, беше проектирана и реализирана от Института по отбрана през последните години[1]. Прототипът на тази информационна среда включва: специализирана подсистема за групова работа; подсистема за комуникация и видеоконференции; документално-информационна подсистема; подсистема за обмен на съобщения и оповестяване; географска информационна подсистема; подсистеми за управление и за защита на информацията и др. Тази информационна среда осигурява следните по-главни информационно-комуникационни услуги:

- ✓ *общ информационен портал*, за споделяне на документи и за публикуване на информация с различни права за достъп върху нея;
- ✓ *видео и аудио конференция* между участници;

- ✓ *IP-телефонни и видеотелефонни услуги* в мрежата;
- ✓ работа с електронни документи и *организиране на документопоток* (създаване, редактиране, одобряване, подписване с електронен подпис, публикуване и отпечатване на документи);
- ✓ *съвместна работа върху общ електронен документ* от физически отдалечени участници в мрежата;
- ✓ *географски информационни услуги* за работа с електронни карти и георeферирана информация;
- ✓ *услуги за съвместно обсъждане на информация* и организиране на брифинги, работни процеси и оперативни мероприятия;
- ✓ *електронно-пощенски услуги (E-mail)* и др.

Тази информационна среда беше демонстрирана в съвместни тренировки по електронни съобщителни средства, проведени в края на 2010 и 2011 г. с участието на структури от МО и БА, няколко министерства и ведомства, областни и общински съвети за сигурност и високо оценена от участниците.

ЗАКЛЮЧЕНИЕ

Намирането на точният баланс между необходими способности и налични ресурси е може би най-сериозното предизвикателство в условията на финансова криза, което изисква постоянно оптимизиране на начертаните приоритети, както и на схемите за финансиране на различните проекти. Важна насока на развитието на въоръжените сили е осигуряване на висока степен на изпълнение на декларираните способности и развитие на нови способности без съществено увеличаване на необходимите за това ресурси. Това може да се постигне чрез ясен, научнообоснован подход за модернизация на въоръжените сили и осигуряването им с ефективни, надеждни и боеспособни въоръжение, системи и технически средства. Институтът по отбрана има силите и средствата да направи това и да даде на ръководството на МО и БА вярна и точна експертиза за състоянието, възможностите и перспективите за изграждане на въоръжените ни сили като част от една модерна, боеспособна и ефективна армия за гарантиране на националния ни суверенитет.

ЛИТЕРАТУРА

1. Илиев, Р., Информационните среди за съвместна работа – средство за подпомагане на управленските процеси, списание „CIO” 48-49 стр., септември 2011 г.
2. Мильов, Й., Военни способности – основа за изграждане и развитие на доктриналната политика на република България, НК, Военна академия "Г.С.Раковски",
http://rdsc.md.government.bg/BG/Activities/Konference/plenarni/Miliov.htm

3. Национална отбранителна стратегия, 2011 г.
4. Националната отбранителна стратегия – баланс на амбиции и необходими отбранителни способности, НК, Военна академия "Г.С.Раковски", http://rdsc.md.government.bg/BG/Activities/Konference/plenarni/Expoze_2010-fin--NK.htm
5. Речник на термините и дефинициите използвани в НАТО (AAP-6)
6. Семерджиев Ц., Информационна война, Софттрейд, С., 2000, стр. 127
7. Семерджиев Ц., Стратегическо ръководство (лидерство), Софттрейд, С., 2000.
8. Симеонов, С., Реформите във въоръжените сили на република България, Пролетна сесия на Парламентарната асамблея на НАТО, 27-30 май 2011 г., Варна
9. Славчев, С. Основи на информационното превъзходство и мрежово центричните военни действия, КР, Военна академия "Г. С. Раковски", 2005 г.
10. Стоянов, Н, С. Балабанов, Кибератаките - новият инструмент в арсенала на армиите, доклад, Кръгла маса"Състояние и проблеми на сигурността в киберпространството на България, СОР "Атлантик" - АКИС, 2010 г. http://www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/docs/programme-28-09-10.pdf
11. https://www.cwid.js.mil/public/CWIDFctShtSuccesses21Mar08.doc
12. http://danysto.info/e-school/courses/C4ISR/22.htm
13. http://www.ezenia.com/news/infoworkspace-saves-lives-in-iraq/
14. http://www.inf.unisinos.br/~cazella/dss/aula7/p51-maybury.pdf
15. Schneider B. R., Principles of War for the Battlefield of the Future, стр.19