

Тодор Тагарев, „Ще се развиват ли способности за информационни операции във Въоръжените сили на Република България?“ Научна конференция на факултет „Национална сигурност и отбрана“ (София: ВА „Г.С. Раковски“, 2007). – под печат.

Todor Tagarev, “Will the Bulgarian Armed Forces Develop Information Operations Capabilities?,” *2007 Annual Scientific Proceedings of the National Security and Defence Faculty, Sofia* (Sofia: “G.S. Rakovski” Defence and Staff College, 2007).

---

---

## **Ще се развиват ли способности за информационни операции във Въоръжените сили на Република България?**

**доц. Тодор Тагарев <sup>1</sup>**

### **Резюме**

Към настоящия момент поставеният в заглавието въпрос няма еднозначен отговор. Тази публикация разглежда развитието на възгледите за информационната война и информационните операции от средата на 90-те години до днес, представени в публично достъпни официални документи и публикации на български автори. В първата половина от този период интересът и концептуалното третиране на въпроса за противоборството в информационната сфера се развиват по възходяща линия. Но при подготовката за членство в НАТО, а в следствие и като член на Алианса, България изглежда затруднена да превърне концептуалните възгледи за информационни операции в съответни способности на Въоръжените сили. Затова втората част на публикацията представя накратко механизма на планиране за способности, чрез който една концепция за операции би могла да се превърне в способности. В заключението се посочва, че отговорът на въпроса, поставен в заглавието, може да бъде положителен, ако България вземе решение да специализира в развитието на способности за изпълнение на една или две съставляващи на информационните операции, след което приеме и изпълни реалистични програми за изграждане и поддържане на тези способности.

### **Развитие на възгледите за информационни операции**

---

<sup>1</sup> Авторът е ръководител на катедра „Мениджмънт на отбраната и Въоръжените сили“ във факултет „Национална сигурност и отбрана“ на ВА „Г.С. Раковски“ и водещ изследовател по въпроси на планиране на силите, мениджмънта на отбранителните ресурси и трансформацията. Статията отразява резултати от научно изследване SfP 981149 на тема “Operations Research Support to Force and Operations Planning in the New Security Environment” („Изследване на операциите в поддръжка на оперативното планиране и планирането на силите в новата среда за сигурност“), финансирано по програмата на НАТО „Наука за мир“. Изразените в материала възгледи са авторски и не ангажират ръководството на ВА „Г.С. Раковски“ или други организации.

В началото на 90-те години на 20-ти Българската армия се оказва без парадигма за развитие след края на Студената война, а ръководството на страната и армията – без опит в планирането на отбраната и управление на развитието на Въоръжените сили с отчитане на измененията в средата за сигурност. По тези причини почти до края на века България се придържаше към организационни решения и оперативни концепции от една отминала епоха, като промените се изразяваха най-вече в механично съкращаване под въздействието на демографски фактори, намаляването на срока на служба на наборните войници и матроси и свиващ се бюджет за отбрана.

При този механистичен подход драстично бяха намалени средствата, а в следствие и организационните единици за провеждане на научни изследвания и поддръжка на развитието на Въоръжените сили. Може би това е обяснението на факта, че официалните структури на Министерството на отбраната и армията реагираха с известно закъснение на т.н. „революция във военното дело” във всичките ѝ компоненти, вече ярко демонстрирани в първата война в Персийския залив, 1990-91 г. Това закъснение бе компенсирано в известна степен от нарасналия достъп на информация чрез Интернет и инициативата на отделни учени и изследователи с интереси към развитието на военното дело и информационните технологии в условията на демократизация на българското общество. Именно стечението на тези фактори доведе до появата на книгата „Информационни аспекти на сигурността”,<sup>2</sup> която всеобхватно разглежда връзката и взаимното влияние между сигурността и развитието на информационните технологии, конфликтите в информационното общество, основни технологии, осигуряващи конкурентни предимства в конфликтите на информационната ера и основните въпроси на управлението на информационната среда.

В книгата, публикувана през 1996 г., Велизар Шаламанов и авторът на настоящата публикация анализират принципите, равнищата, сферите и компонентите на информационното противоборство и определят *информационната война* като

Система от действия, предприети да създадат информационно пространство, в което едната страна има превъзходство в разбирането и използването на силните и слабите страни в политическата, икономическата, военната, социалната и културната области на действие на потенциалния противник и зависимостта му от приятелски източници на мощ, като в същото време не се допуска ефективност в аналогичните действия от негова страна.<sup>3</sup>

---

<sup>2</sup> Велизар Шаламанов и Тодор Тагарев, *Информационни аспекти на сигурността* (София: Прокон, 1996 г.).

<sup>3</sup> Пак там, стр. 82-83.

Авторите идентифицират информацията като отделна сфера, мощно оръжие и изгодна цел в развитието на конфликта и определят термина „*информационна мощ*” като потенциал, създаван от модерни технологии, адекватни процедури и организационни решения. Освен това, те разглеждат *информационната кампания* като основното средство, използвано в комбинация с традиционни военни средства и методи, за постигане на информационно превъзходство, и разглеждат детайлно две равнища на тази кампания:

- Стратегическа информационна кампания, насочена към постигане на парализа на НОРД<sup>4</sup> цикъла на опонента, и
- Борба за превъзходство в управлението (военния аспект на информационната война), поддържаща постигането на стратегическите цели чрез въздействие върху способностите на противника да взима навременни и адекватни решения за използване на собствените си въоръжени сили.

Шаламанов и Тагарев определят шест основни елемента на операцията за постигане на информационно превъзходство:

1. Сигурност на операциите – възпрепятстване на получаването от страна на противника на информация за нашите намерения и действия чрез гарантиране сигурност на комуникациите, компютърна сигурност, контрол на излъчванията и т.н.;
2. Маскировка;
3. Психологически операции;
4. Електронна война;
5. Физическо въздействие върху елементи на противниковата C4ISR система;
6. Превъзходство в разбирането за ситуацията чрез ефективно разузнаване и обобщаване на информацията от всички източници.

Освен това, авторите разглеждат атакуващия и отбранителния аспект на информационните операции, ролята на медиите и информационните аспекти на операции, различни от война.

Автор на предговора към книгата генерал Михо Михов—тогава Началник на Главния щаб на ВВС, а по-късно (1997-2002 г.) Началник на Генералния щаб на Българската армия—представя своите възгледи за ролята на информацията в съвременния конфликт,<sup>5</sup> в това число:

---

<sup>4</sup> Наблюдение – ориентация – решение – действие, в англоезичната литература известен като *OODA loop*.

<sup>5</sup> Генерал Михо Михов, “Информация и национална сигурност,” предговор към Шаламанов и Тагарев, *Информационни аспекти на сигурността*, стр. 5-7.

- Театърът на военните действия вече не се съизмерва географско-физически с класическия ТВД, а все повече навлиза в информационната сфера;
- Информационното превъзходство е средството, с което може да се разубеди даден противник, да се отложи агресията и дори да се предотврати война;
- Победата в информационната война предопределя изхода на класическите военни действия;
- Необходимо е да се намери нов баланс между огневата мощ и информационната мощ;
- България няма алтернатива на подготовката за информационна война.

С последвалата серия от статии в списание „Военен журнал” и други официални издания на МО и БА авторите допринесоха за повишаване на вниманието към и разбирането за измененията в конфликтите в информационната ера, информационните операции и дебата относно използването на модерни информационни технологии в рамките на нови оперативни концепции, както и за приоритетите в развитието на въоръжените сили.<sup>6</sup>

Приз 1998 г. в условията на нарастващия интерес към взаимната обусловеност между сигурността, военното дело и съвременните технологии, особено информационните технологии, авторите на книгата инициираха издаването на списание “*Information & Security: An International Journal*” с идеята то да отразява “научни, технически и организационни въпроси, свързани с националната и международна сигурност в информационната ера, C4ISR технологии и системи, информационните операции, борбата за превъзходство в управлението и информационната сигурност.” Декларираната цел на списанието бе то “да хвърли мост между технологичната общност и общността на експерти по въпроси на сигурността, като представя съвременното равнище, нови идеи, технологии и потребности на всяка от двете мощности, както и нови изследователски и практически резултати на стика между двете общности.”<sup>7</sup>

Генерал Михов—по това време вече Началник на Генералния щаб на Българската армия—публикува статия в първия брой на списанието.<sup>8</sup> В тази статия той разглежда концепцията за информационната война и информационните операции в контекста на реформата на Българската армия и разглежда информационната война на две равнища – стратегическо и оперативно. Основна теза на генерал Михов в тази статия е, че

<sup>6</sup> Вж. например Тодор Тагарев, Към създаването на теория на информационната война, *Военен журнал*, т. 104 (1997), бр. 4, стр. 52-58; Велизар Шаламанов и Тодор Тагарев, Информационната война и борбата за превъзходство в управлението, Сборник трудове на ВА "Г.С. Раковски", кн. 5, 1997 г., стр. 51-71.

<sup>7</sup> Вж. <http://infosec.procon.bg>.

<sup>8</sup> Генерал Михо Михов, “Българската армия в Информационното общество,” *Information & Security: An International Journal* 1:1 (Summer 1998): 15-25.

информационната операция се превръща в основна поддържаща, а „в перспектива и в *основна самостоятелна операция* на Въоръжените сили , провеждана в тясно взаимодействие с други държавни и обществени организации.”<sup>9</sup> В статията се използва следното определение за информационна операция:

Система от действия за създаване на информационно пространство, в което едната страна има превъзходство в разбирането и използването на силните и слабите страни в политическата, икономическата, военната, екологичната, социалната и културната области на действие на потенциалния противник и зависимостта му от приятелски източници на мощ, като в същото време не се допуска ефективност в аналогичните действия от негова страна.

Като цел на информационната операция генерал Михов определя постигането на крайно епистемологично състояние, т.е. промяна в начина на разсъждение и вземане на решение от противника в желаната от нас посока, а необходимо условие за това е постигането на информационно превъзходство. Информационната операция се провежда в комбинация с традиционни методи и средства за въздействие върху противника, а при планирането ѝ трябва да намери отговор въпроса как тя се съотнася към общите цели на войната или операцията, какво бихме искали да знаят, мислят и вярват противниковите лидери след приключване на информационната операция и как по най-добър начин бихме могли да удовлетвори критериите за успех.

По стечение на обстоятелствата и тримата споменати автори имаха важна роля в процеса на разработване на първата национална военна доктрина<sup>10</sup> – генерал Михов като Началник на Генералния щаб, д-р Шаламанов като заместник министър на отбраната по военната политика и планирането и д-р Тагарев като директор на дирекция „Планиране на отбраната” в МО. Имено Военната доктрина бе първият официален документ, третиращ въпроса за информационните операции и други информационни аспекти на сигурността. Така например, доктрината нарежда информационната война сред съвременните рискове и заплахи за сигурността (чл. 9 и чл. 11) и определя провеждането на „информационни атаки от страна на чужда държава срещу национални стратегически системи” като инструмент за въздействие срещу страната в условията на военнополитическа криза и военен конфликт (чл. 16). За първи път бе поставена задача за постигане на информационно превъзходство. Съгласно чл. 62 „Въоръжените сили осъществяват отбраната на страната чрез прилагане на военностратегическа концепция за

---

<sup>9</sup> Пак там, стр. 21.

<sup>10</sup> *Военна доктрина на Република България*, приета с решение на Народното събрание от 8 април 1999 г., изменена и допълнена с решение на Народното събрание от 22 февруари 2002 г., Държавен вестник, бр. 20 от 2002 г.

защита на националната територия, борба за информационно превъзходство, контрол на въздушното и морското пространство и отбрана на застрашен театър на военните действия”. Респективно, приоритет в модернизацията на въоръжените сили получиха „системите за командване, управление, наблюдение, разузнаване, комуникации, взаимно опознаване, компютризация, навигация, включително с космически системи, средства и технологии” (чл. 97).

Военната стратегия на Република България повтори много от постановките на военната доктрина, включително задачата за постигане на информационно превъзходство, и посочи информационната операция като част от съвместната стратегическа отбранителна операция.<sup>11</sup>

В периода 1999 – 2002 г. бяха разработени значителен брой нови доктринални документи и значителна част от тях съдържаха постановки, пряко третиращи въпроса за информационните операции или свързани с тях положения. Доктрината за съвместните операции от 2001 г. в част III „Съвместните операции при военен конфликт” съдържа раздел „Информационни операции (операции срещу системите за командване, управление, компютеринг и разузнаване – С4I)”,<sup>12</sup> като разглежда следните основни компоненти: сигурност на операциите; дезинформация, маскировка и заблуда на противника; психологически операции; електронна война; огнево поразяване (физическо унищожаване). В нея информационните операции се определят като „съвкупност от съгласувани по цели, задачи, място и време информационни въздействия, атаки и сражения, провеждани по единен замисъл и план за решаване на задачи на информационната борба на театъра на военните действия или на оперативни направления”. Развита е постановката за поддържащата роля на информационните операции чрез „въздействие върху способността на противника да взема навременни и ефективни решения за използване на своите въоръжени сили”. Определени са и двете им съставни части: защитна (запазване на ефективността на собствените системи за командване и управление) и въздействаща (възпрепятстване, разстройване и разрушаване на системите за командване и управление на противника). Освен това, доктрината възлага на Оперативно управление (J3) да координира, планира и да поддържа ръководството на всички основни компоненти на информационните операции, а на Управление „Комуникационно-информационни системи” (J6) – да организира защитата на информацията от преднамерени въздействия.

Доктрините на видовете въоръжени сили разглеждат отделни елементи на информационните операции, а документът „Основни насоки за оперативно планиране”

<sup>11</sup> *Военната стратегия на Република България* (София: Генерален щаб на Българската армия, 2002 г.).

<sup>12</sup> *Доктрина за съвместните операции* (София, Генерален щаб на Българската армия, 22 февруари 2001 г.).

предвижда отделни приложения към плановете за операциите за информационни операции, психологически операции и електронна война.<sup>13</sup>

Още трима български автори имат особен принос към поддържането и развитието на интереса към информационните операции. През 2000 г. проф. Цветан Семерджиев публикува книгата „Информационна война.“<sup>14</sup> Изчерпателно авторът анализира рисковете и заплахите на националната сигурност на прага на третото хилядолетие, особено произтичащите от разпространението на информационни технологии и комуникационни канали, въвежда концепцията за „национално информационно пространство“ и необходимостта да се организира неговата ешелонирана отбрана. Проф. Семерджиев представя детайлно концепцията за *информационна мощ* и прилага класически принципи на войната за изведе принципите на информационната война и използването на съвременни информационни технологии.

През 2003 г. полк. Митко Стойков публикува книга за връзката между информационната революция и тероризма и значението ѝ за организиране на системата за сигурност.<sup>15</sup> В книгата се представят концепциите за кибернетична война, информационна война и мрежова война на основата на сравнителен анализ на предимно американски източници. Главата за информационните операции<sup>16</sup> се основава изключително на източници от Пентагона – Съвместната доктрина за информационни операции (Joint Pub 3-13, Joint Doctrine for Information Operations), полевия устав на Сухопътни войски на САЩ FM 100-6; и доктрината за комуникационна поддръжка на съвместни операции (Joint Publication 6-0, Doctrine for Communications System Support to Joint Operations).

Може би това е последния към момента пример на комплексно, системно третиране на въпроса за информационните операции от български автор. Основната причина е, че докато процесите на значително съкращаване продължаваха, след срещата на върха във Вашингтон България прие План на действие за членство в НАТО,<sup>17</sup> а на срещата в Прага през 2002 г. получи покана да се присъедини към Алианса. При подготовката си за членство България трябваше да изпълни значителен брой разнообразни по характер изисквания. Най-голямо значение за промените в информационната сфера имаха изискванията за оперативна съвместимост и защита

<sup>13</sup> *Основни насоки за оперативно планиране* (София, Генерален щаб на Българската армия, юли 2000 г.).

<sup>14</sup> Цветан Семерджиев, *Информационна война* (София: Софттрейд, 2000 г.). Допълнително третиране на въпроса за информационните операции авторът прави в Цветан Семерджиев, „Информационна сигурност,” в *Национална и международна сигурност*, под ред. на Валери Рачев с колектив (София: Военно издателство, 2005 г.), стр. 275-298.

<sup>15</sup> Митко Стойков, *Информационната парадигма в системата за сигурност и тероризма* (София: Военно издателство, 2003 г.).

<sup>16</sup> Пак там., стр. 80-85.

<sup>17</sup> A country with acknowledged ambitions for NATO membership and respective Membership Action Plan (MAP).

на класифицираната информация. В комбинация с други ограничения, тези изисквания се оказаха прекомерни за капацитета на военното ведомство за планиране и мениджмънт на силите.

Все пак, през юли 2007 г. се появи нова публикация на бригаден генерал Бойко Симитчиев<sup>18</sup> – началник на управление „Комуникационно-информационни системи” на ГЩ и Главен информационен мениджър на Министерството на отбраната, с която авторът отново връща по-широкия интерес към информационните операции и подчертава, че предизвикателствата на информационните операции в условията на трансформация и модернизация е с „особено важно значение за насочване на нашите усилия по създаване и генериране на необходимите способности на Българската армия за *участие в мисии на НАТО и Европейския съюз*”. Генерал Симитчиев набляга на нарастващото значение на информационното превъзходство и на ролята на психологическите операции за спечелването на симпатиите на местното население в операции от различен характер. В заключението си авторът отбелязва, че подготовката за информационната война е без алтернатива, а от първостепенна важност е успешното ни участие в бъдещи информационни операции.

Подготовката за информационната война, и в частност дали Въоръжените сили на Република България ще участват в информационни операции и успехът на това участие зависят най-вече от това, дали ще се вземат рационални, реалистични решения за изграждане на съответни способности.

### **За превръщането на изисквания в способности**

Една нова концепция за операции, например за информационни операции, е от практическо значение, само ако намери адекватното си място в процеса на планиране на отбраната и въоръжените сили и доведе до развитието и поддържането на съответни способности.

При планирането за способности—основният подход към планирането на силите, прилаган от НАТО, Европейския съюз и повечето от страните членки—необходимите способности се определят спрямо задачите, които се възлагат на силите за изпълнение и условията, в които ще се изпълняват тези задачи. Най-общо, способността се определя от капацитет, създаван от наличието на умения и материални средства, да се реши определена задача. Според едно по-прецизно определение, използвано в планирането на силите, носител на способността е съответна комбинация от умения и ресурси, осигуряващи *инструменти* за

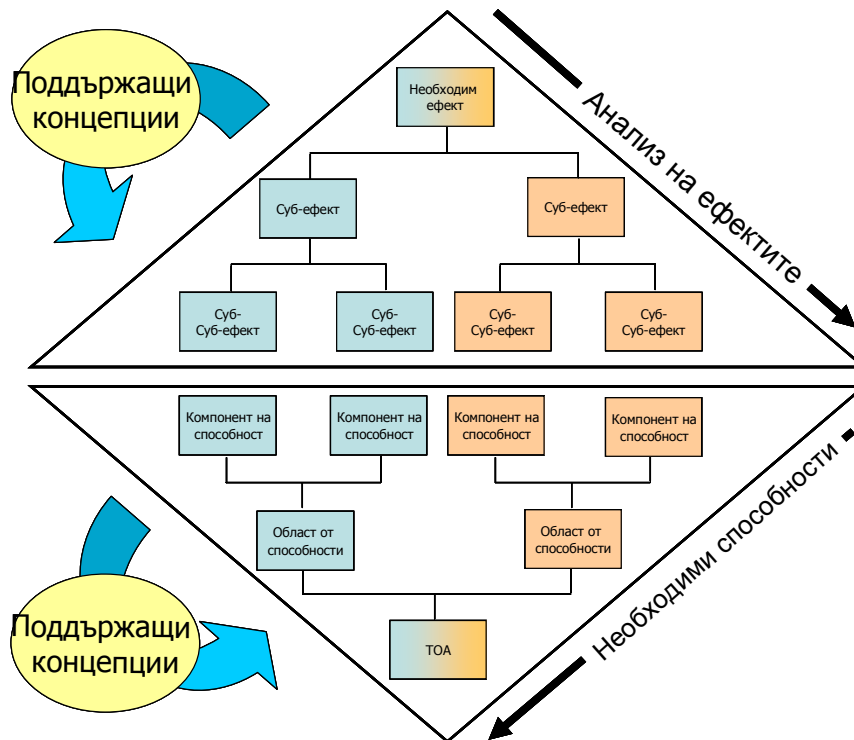
---

<sup>18</sup> Бригаден генерал Бойко Симитчиев, “Информационните операции и предизвикателствата на бъдещата война,” *CIO.bg*, бр. 7 (юли 2007 г.).



постигане на *измерим резултат*, при изпълнение на *определени задачи*, в *конкретни условия* и при съблюдаване на зададени *стандарти*.<sup>19</sup>

Задачите могат да бъдат изпълнявани по различни начини. В планирането на силите този факт се отчита чрез включване в процеса на планиране на силите на предвиждани *концепции за операции*, например концепцията за информационни операции. Тези концепции определят въздействието (или *ефекта*), което бихме желали да постигнем за да изпълним възложените задачи. Това въздействие се декомпозира, а декомпозицията се използва за да бъдат определени компонентите на необходимите способности (вж. фигурата по-долу).<sup>20</sup> Един възможен пример е определяне на необходими способности за атака срещу компютърни мрежи на противника в рамките на концепцията за информационни операции.



Фигура 1: Определяне на необходими способности и области на трансформация (ТОА - Transformation Objective Areas)

<sup>19</sup> Todor Tagarev, "The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithm)," Connections: The Quarterly Journal 5:1 (Spring-Summer 2006): 15-34, [https://consortium.pims.org/filestore2/download/3472/The Art of Shaping Defense Policy.pdf](https://consortium.pims.org/filestore2/download/3472/The%20Art%20of%20Shaping%20Defense%20Policy.pdf).

<sup>20</sup> Вж. например, Niels Driis, Allied Command Transformation, "NATO Transformation and the Challenges for Defence Planning," presentation to the seminar *Harmonization of National Defence Planning with NATO Defence Planning* (Sofia, October 2004).

След това способностите—на равнища, определени в процеса на планиране на силите—се създават чрез въвеждане на адекватни процедури, или доктрина, организационни структури, личен състав, подготовка и материални средства.

Прилагането на процес на планиране от описания вид представлява изключително предизвикателство, особено имайки предвид разнородните по характер изисквания за подготовка на членство в НАТО и изпълнение на цели на въоръжените сили (Force Goals), участието в операции, процеса на професионализация, фокуса върху закупуването на основни платформи оръжия през последните години и продължаващия процес на намаляване на бюджета за отбрана и съкращаване на личен състав. Именно в такива условия поддръжниците на информационните операции би следвало да се преборят за адекватно финансиране. Няма данни до момента те са постигнали сериозни успехи.<sup>21</sup>

Въпреки това, изграждането на способности провеждане на елементи на информационни операции във Въоръжените сили на Република България е както необходимо, така и възможно при един реалистичен подход, основан на следните положения:

Първо, желателно е да се ограничим в използването на термина „информационни операции” до неговото военно значение, заложено в съюзните документи.

Второ, Въоръжените сили на Република България могат да *допринасят* към операции на НАТО, Европейския съюз или водени от съюзник коалиции, в частност информационни операции, като прилагат съюзните политики, доктрини и концепции за информационни операции, а не се стремят към създаването, и особено към прилагането на уникални концепции. При това България може да допринася за развитието на съюзните възгледи за информационните операции чрез участие в научни изследвания, развитие на концепции и провеждане на експерименти, разработване и производство на технологични решения.

Трето, едва ли бихме могли да се стремим към развитие на широк спектър от способности за провеждане на информационни операции. Реалистично е България да *специализира* в развитието и използването на един или два типа способности, например в атакуването и защитата на компютърни мрежи. От особен изследователски интерес в това отношение е как да се създадат типови подразделения, които да са относително самостоятелни и със ценен принос към многонационални операции.

---

<sup>21</sup> Според вестник „Българска армия”, бр. 16310 от 06.03.2006 г., отделни български офицери от групите за връзка и наблюдение (LOT) изпълняват и задачи, свързани с информационни операции (Вж. „Концепция, която работи втора година, LOT показва пред местните хора приятелското лице на EUROFOR”), но едва ли това може да се определи като „способности на Въоръжените сили за информаиционни операции”.

Четвърто, целесъобразно е атакуващата (или „въздействащата“) част на информационните операции да се подчини на развиващата се концепция за *операции, ориентирани към целево въздействие* (или Effects-Based Operations),<sup>22</sup> а България да се включи в съответните изследователски проекти и експерименти в рамките на НАТО.

И пето, докато защитата на собствената система за командване и управление се разглежда като част от отбранителните информационни операции, други елементи от информационната инфраструктура също могат да имат критично значение за сигурността на държавата и обществото. Очаква се защитата на тази инфраструктура (на територията на страната) да се организира в рамките на политиката на Европейския съюз за защита на критичната инфраструктура,<sup>23</sup> като България оцени в каква степен да разглежда системата за управление в кризисни ситуации като елемент на критичната инфраструктура.<sup>24</sup>

В заключение още веднъж ще подчертаем, че развитието на способностите за информационни операции би трябвало да получи приоритет в развитието на Въоръжените сили. Но не е достатъчно само да се направят декларации в този смисъл. За да има положителен отговор на поставения в заглавието въпрос, ръководството на Въоръжените сили трябва да вземе решение за *специализация* на България в развитието на способности за изпълнение на една или две съставляващи на информационните операции, и това решение да бъде последвано от приемане и изпълнение на реалистични програми за изграждане и поддържане на тези способности. Това може да бъде забележим и престижен принос на България към усилията на НАТО и Европейския съюз в борбата с тероризма и за повишаване на стабилността и сигурността в света.

---

<sup>22</sup> Вж. *CONOPS Information Operations (Info Ops) Planning for Effects-Based Operations*, Version 1.0 (Multi-national Information Operations Experiment, October 2004).

<sup>23</sup> Вж. например *Critical Infrastructure Protection in the Fight Against Terrorism* (COM(2004) 702 final), October 2004; *Protection of Critical Infrastructure*, European Parliament recommendation on the protection of critical infrastructure in the framework of the fight against terrorism (2005/2044(INI)), C 124 E/250-253, 25 May 2006; *Green Paper on a European Programme for Critical Infrastructure Protection* (COM(2005)576 final), (Brussels: Commission of the European Communities, 17 November 2005); и *EU strategy to protect critical infrastructure from terrorist attacks*, Resolution of the European Parliament, 10 July 2007.

<sup>24</sup> Към момента Европейският съюз не предвижда експлицитното ѝ включване като елемент на критичната инфраструктура. Вж. *Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection*, Commission proposal COM(2006)787 final, December 2006.