БЪЛГАРСКА Наука

ISSN:1314-1031 ФЕВРУАРИ 2019

СПЕЦИАЛЕН БРОЙ НАЦИОНАЛНА СИГУРНОСТ

АБОНАМЕНТ

СП. БЪЛГАРСКА НАУКА

25 лв. за година

БЪЛГАРСКА НАУКА
НАУЧИ ПОВЕЧЕ

АВТОРИ В ТОЗИ БРОЙ:
Полк. доц. д-р Петко Димов
Полк. доц. д-р инж. Галин Иванов
Майор асистент Живко Лавчев
Майор Валентин Иванов Георгиев
Полк. доц. д-р Тотко Симеонов
Полк. Владимир Кабаиванов
Подполковник д-р Живко Желев
Подполковник д-р Милен Кисьов
Полк. доц. д-р Иван Чакъров

ДИЗАЙН:
Петър Теодосиев

КОРИЦА:
pixabay.com
Петър Теодосиев

КОНТАКТ:
Петър Теодосиев - admin@nauka.bg
0885811386

6 ПРИЧИНИ ДА ПУБЛИКУВАТЕ В СП. БЪЛГАРСКА НАУКА

ШРИФТОВЕ:
Fontfabric

СНИМКИ:
Public domains

СЪДЪРЖАНИЕ

НАЦИОНАЛНА СИГУРНОСТ

ЕДИН ПРОЕКТ НА "БЪЛГАРСКА НАУКА"

СЛУШАЙ НАУКА

Изчетени статии от сайта и списанието БГ Наука (www.nauka.bg)

Брой 1 • www.nauka.bg/slushai

MOVE.BG

Заедно променяме България

БГ Наука Подкаст:

Слушай през **Android**
Слушай в **iTunes**
Слушай в **Nauka.bg**
Слушай в **STITCHER**

Анализ на потенциалните възможности за предизвикване на нова световна война

Автор: Полк. доц. д-р Петко Димов

Анотация: В статията се дефинират общите закономерности, чрез които се повтарят зараждащите се световни конфликти. Въз основа на анализа на тези закономерности и съвременната геополитическа обстановка е направен опит за разпознаване на държавите, които е най-вероятно да предизвикат трета световна война.

Ключови думи: световна война, геополитика, *национална сигурност*

The article defines the patterns that cause global conflicts. An attempt has been made to uncover the countries most likely to trigger a third world war.

***Key words**: World War, Geopolitics, National Security*

Един от основните научни проблеми при идентифицирането на потенциалните източници за започване на трета световна война е, че съществуват само две исторически точки за сравнение, които са предизвикали световни войни в миналото. Първата световна война и Втората световна война имат

различен генезис и различни цели, но освен това имат редица прилики, които показват как регионалните конфликти могат да се превърнат в световна война. В настоящата статия е направен опит да се намерят общите закономерности, чрез които се повтарят зараждащите се световни конфликти, както следва:

1. Наличие на несигурни съюзи. И двете отминали световни войни започват с подценяване и недоглеждане на съюзните структури. Днес в съвременния свят военните съюзи и гаранции ни изглеждат очевидни, но през 1914 г. и през 1939 г. надеждността на съюзните договорки е била абсолютно несигурна. Тази несигурност е основен фактор, допринасящ за получаването на световна война. Държавите обявяващи война на други държави, не вярват, че съюзниците на нападнатите ще им дойдат на помощ. Например, нахлуването на нацистка Германия в Полша през 1939 г. предизвика лавинообразно обявяване на нови декларации за война от други страни, докато Хитлер е вярвал, че това не би довело до по-голяма световна война.

2. Намеса на „Великите сили“. Ако разгледаме историята на противопоставянето между Германия и Великобритания, САЩ и Япония или историята на Балканските държави, лесно ще забележим стремежа на „Великите сили“ да ограничават експанзията на потенциални съперници. Глобалните

Полковник доцент доктор Петко Димов е началник на секция „Иновации и платформи в образованието и квалификацията“ на Институт „Перспективни изследвания за отбрана“ към Военна академия „Г. С. Раковски“.

сили използват принципа „разделя – владей“ за да създават малки конфликти в точките, където може да се зароди друга глобална сила.

3. Нерешени конфликти между съседни държави. Историята показва, че повечето досегашни войни се водят заради останали нерешени проблеми от предишната война[1].

С помощта на тези три исторически закономерности можем да разгледаме съвременните потенциално опасните райони, където местните конфликти могат да излязат извън контрол. Тъй като днес има един глобален съюз - Организацията на Северноатлантиче-

ския договор (НАТО) и една глобална сила САЩ, то е много вероятно, ако има нова световна война точно те да участват в нея[2]. Освен това едно такова участие е свързано с използване на последните образци въоръжение и техника на промишлените комплекси на страните с тестване в реални условия на възможностите им[3]. За нуждите на анализа трябва да разгледаме геополитическата карта на света и да намерим горещите точки в които те имат интереси и съществуват нерешени отминали конфликти.

Страните от Близкия Изток

Войната в **Сирия** има потенциал да се превърне в нова световна война, защото притежава и трите гореописани закономерности: много исторически нерешени проблеми, наличие на несигурни съюзи и интереси на Великите сили. В нея са намесени всички съвременни глобални и регионални сили, както и нашите съседи от юг, което може да доведе до опасни последици за нашата страна. От една страна са Русия и Иран, които помагат на правителството на Башар Асад, от друга е местната опозиция близка до САЩ, Саудитска арабия и Турция[4]. От трета страна там действа **„Ислямска**

държава“, която със сигурност е заплаха, както за националната така и за съюзната сигурност на страните от Европейския съюз. Нещо повече, „Ислямска държава“ официално декларира, че основна и цел е да предизвика трета световна война на Исляма срещу Запада, което е класически сблъсък на цивилизациите. Този сценарии е малко вероятен, защото като цяло за съвременния човек национализма е по-силна идеология, отколкото религията и това затруднява индивидуалните ислямските народи да се обединят само заради общата вяра. Освен това, никой от тях към момента не притежава конкурентни на запада военно въздушни сили за влияние извън региона. Въпреки това борбата с „Ислямска държава“ се води с противоречиви резултати тъй като интересите на САЩ и Русия са в противоречие.

Докато в Сирия борбата е много заплетена в Ирак американците разчитат на кюрдите и шиитската милиция. Това доведе до охладняване на отношенията между САЩ и Турция, която започна да води собствена политика на неосманизъм в региона. Стария конфликт на република Турция с „Кюрдската работническа партия – ПКК“ е отнел живота на повече 30 000 души. Днес той е в пълна сила. Кюрдите се опитват да създадат собствена автономия в Сирия и Ирак, което притеснява Турция, че това ще повлече и турските кюрди. Поради тази причина се проведе операция „Щит на Ефрат“, турската армия навлезе в Сирия и усложни още повече обстановката там.

При евентуално влизане на някоя от другите големи регионални сили и предизвикване на война между **Саудитка арабия и Иран**, тази война ще премине на друго световно ниво. Саудитска Арабия има третия по големина военен бюджет в света. Мюсюлманската реторика, която излиза от там е също толкова войнствена колкото на „Ислямска държава“, но повече от това те мразят Иран. От своя страна Иран притежава ядрено оръжие и имат военен потенциал на нивото на Турция. Това кара Саудитската кралска кръв бързо да кипва и е възможно да обявят война на Иран покрай вече зародилия се конфликт. Това неименуемо ще въвлече САЩ на страната на Саудитска арабия, защото според тях Иран са част от оста на злото, а Иран е в съюз с Русия и Китай. От там при разрастване на подобен конфликт със сигурност се намесват всички страни от НАТО и войната става световна.

Освен горните проблеми в Близкия изток нараства и напрежението между Ирак и Саудитска арабия. Също така конфликта в **Йемен** е един от най-новите и от март 2015 до сега е отнел живота на повече от 7 000 души и 40 000 ранени. Там се води въстание на шийти срещу правителството подкрепено от Саудитска Арабия. Друг евентуален

конфликт между Иран и Израел също може да доведе до ядрена война.

Друга гореща точка в региона е **Афганистан**, който остава в същото положение, каквото е бил в последните 40 години. След намесата на САЩ за сваляне на талибаните те все още са сила и дори към момента започват постепенна офанзива в някои райони на страната. Това е едната от причините тази страна да е втория донор за износ на бежанци към Европа след Сирия. България участва с военен контингент в операция Resolute Support в подкрепа на афганистанските сили, заедно с 9800 американски войници, поради което има опасност, както за военнослужещите така и за националната сигурност на страната.

В **Либия** след свалянето на Муамар Кадафи през 2011 се водят жестоки междуособици между няколко фракции, които се бият за нейните богатства. Това също я прави една от основните страни формиращи бежанския поток към България и Европа.

Страните от Индийския океан

Индийския океан е не по-малко взривоопасно място от Близкия Изток. Такъв до голяма степен е и случаят с Източнокитайско море и островите Сенкаку, които могат да предизвикат война между **Китай и Япония**. Там се оформя едно противопоставяне от една страна на коалиция между Индия, Виетнам и Япония срещу Китай и Пакистан. В интерес на истината исторически погледнато повечето войни се предизвикват от бързоразвиващите се държави като Бразилия, Индия и Индонезия, които променят баланса на силите в световния ред.

По-специално, може да се получи голям конфликт за власт между **Индия и Пакистан**, който да предизвика Китай и САЩ, като съюзници с не много изяснени политически договорни отношения. Всъщност, има сходна динамика между Афганистан, Пакистан, Индия Китай и Непал, както и няколко спорни граници в Кашмир, които биха могли да предизвикат световна война, като въвличат глобалните сили.

Съществуват прогнози, че през 2030 г., Китай ще бъде най-голямата икономика в света, следван плътно от Индия. При това положение лидерите на Китай биха искали да имат по-важна роля в световния ред, може би повече отколкото САЩ имат сега. В същото време, Индия ще се нуждае от много повече износ в световната търговия, за да намали все още съществуващи бедни райони на страната.

Пакистан е единствената ядрена сила с нестабилно правителство и идеалното място за наличие на групи от терористи. Ако избухне някакъв голям атентат в Индия, то нейното правителство няма да знае дали това е един терорист или поръчка на правителството на Пакистан. Отговорът ще бъде толкова бърз, колкото е бил

и в Първата световна война, когато Австро-Унгария обявява война, след като ерцхерцог Франц Фердинанд е убит от терористи. Освен това в предишните Индо-Пакистански войни Израел многократно е помагал на Индия и със сигурност ще се включи, особено ако някоя друга ислямска нация се присъединява към Пакистан. Този акт ще предизвика намесата на Китай. Когато Индия започне да се задушава от хватката на Китай ще изпрати емисари в САЩ и Япония. Тъй като днес световната търговията се извършва основно по океанските маршрути за САЩ и Япония е особено важно да не позволяват на Китай да доминира в Индийския океан. С намесата на САЩ и Япония, Русия може да бъде принудена да вземе страната на Китай. По този начин ще се получи троен съюз между Русия, Китай и Пакистан от една страна и САЩ, Япония и Индия, от друга страна.

Друга такава точка в която са налице и трите конфликтни закономерности може да бъде **Тайван**, който има двусмислен договор за отбрана със САЩ, съществуват редица нерешени властови проблеми между Китай и Тайван, между САЩ и Китай и т.н. Това не означава, че ще доведе до световна война, но че този район притежава всички качества да се превърне в голям конфликт.

Украйна и Балтийските държави

Друга изключително близка до нас точка, която може да предизвика световна война е **Украйна**. Тя се намираше до скоро в Руската сфера на влияние, но след разпада на СССР остана само един хегемонен съюз и това даде възможност на нахлуване на западно влияние, което доведе до огромна политическа криза и предизвика гражданска война. Обраузваха се проруските Логантска и Донецка народни републики, а Русия анексира Кримския полуостров.

Все пак през 2017 Украйна сключи споразумението за асоцииране с ЕС и кандидатства да влезне в НАТО до 2020 г., което налага известен сдържащ ефект на Русия. Той може да трае поне до тогава, докато САЩ и ЕС се чувстват по-силни от постепенно стабилизираща се Русия. В момента НАТО има 28 страни членки, за разлика от началото когато са били 12, някои от новите членове са Латвия, Литва, Естония, Чехия и България, които са били във „Варшавския договор“ и това прави Русия враждебна към разширяването на НАТО. Поради тази причина НАТО и САЩ започнаха разполагане на голямо количество военни средства и съвместни военни учения в Източна Европа. Въпреки, че това е по-скоро мярка за безопасност, Русия ги възприема отрицателно и от своя страна увеличава въоръжените сили в граничните райони и образу-

ва нови буферни държави между нея и НАТО. Допълнително изостряне на отношенията между НАТО и Русия със сигурност ще доведе до Трета световна война в която България отново ще се намира на пограничната зона.

Подобна геополитическа динамика съществува в Балтийските държави **Естония, Латвия и Литва**. Има огромен дисбаланс на силите между тези държави и съседна Русия. Русия също се опитва да се утвърди като глобална сила, въпреки опитите на САЩ и ЕС да я ограничат с различни санкции. Докато НАТО е доста стабилен съюз, а тези малки държави са негови членове, евентуални действия там ще ангажират САЩ, Великобритания, Канада, Франция и Германия, като гаранти на Балтийската сигурност. Поради тази причина днес в региона се провеждат редица допълнителни мисии на НАТО, което прави по-малко вероятно Русия да рискува с тези държави.

Северна Корея

Северна Корея е малка ядрена страна с която дори и най-малкия сблъсък може да доведе до ядрена война. В тази конфликтна точка също има наличие и на трите закономерности за започване на световна война: наличие на нерешени конфликти от предишните корейски войни, несигурни политически договорки зависещи от едноличното решение на някой диктатор и икономически интереси на глобалните сили. Северна Корея разработва ядрено оръжие и евентуалната му употреба задължително ще предизвика помощ от други страни включително Китай. А както видяхме по-горе след включването на тази страна ще последва развитие по аналогия на гореописания сценарии.

В страните от централна и **Западна Африка** действа близката до „Ислямска държава“ терористична групировка „Боко Харам“. В Сомалия действа „Ал-Шаба“, клон на „Ал-Кайда“. Много е вероятно при неуспех в Сирия и Близкия Изток, Ислямска държава да насочи фокуса си към Африка. Там на картата се появи и най-новата държава в света Южен Судан, която още е в нестабилно положение и продължават да се водят много вътрешни битки, което отговаря на горните три условия.

В заключение няма да се учудите, че война е възможно дори на **Антарктида**. Този малко известен континент също има конфликти между много страни най-вече за разпределението на земя и ресурси. Русия твърди, че е собственик на повече от половината от Антарктида, включително Северния полюс и е започнала да изгражда свои военни бази в арктически регион и да подготвя войски за действие в арктически условия. Това може да доведе до размирици в страни като Норвегия (член на НАТО), която реагира на това чрез повишаване на тяхната

военна готовност в арктическия регион. Този факт също може да доведе до конфликт между Русия и НАТО, които и без друго постепенно изострят своите отношения. А представяте ли си още кой ще се включи при евентуално откриване на някакви скъпоценни суровини в ледовете на континента?

Много е трудно да се предскаже такова геополитическо събитие, при наличието на което със сигурност да започне война. Историята показва, че това се случва след поредица от непредвидими събития, които обикновено предизвикват локален конфликт. За да се получи световна война трябва да участват световни сили, които контролират големи части от света и предизвикват по-малките да участват. В крайна сметка няма вечни приятели, а има вечни интереси.

(Endnotes)

1 Иванов, Г. Съвременната геополитическа значимост на черноморския регион и мястото на Република България в нея, Годишник на факултет „Командно-щабен“, Военна академия „Г. С. Раковски“, ISBN 1312-2991, София, 2010, с. 205-217

2 Farley, R. 5 Places Where World War III Could Start in 2019, The National Interest, 2019

3 Душков Г. И., Т. Д. Краев, Въоръжените сили в условията на XXI век – развитие и възможности за използване, годишна научна конференция „Използване на въоръжените сили в съвременните конфликти”, 20-21.05.2015 год., ВА „Г. С. Раковски“.

4 Димов, П. Желев, Ж. Анализ на съвместната операция на Руските Въоръжени сили в Сирия, сп. Военен журнал на „ВА Г.С. Раковски“ София, ISSN 2534-8388, 2016, бр.1 стр. 58-67

АБОНАМЕНТ

СП. БЪЛГАРСКА НАУКА

НАЛОЖЕН ПЛАТЕЖ

Предизвикателства пред .....

Автор: Майор асистент Живко Лавчев

ПРЕДИЗВИКАТЕЛСТВА ПРЕД .....

Майор асистент Живко Лавчев

Анотация: Политико-икономическата среда в световен, европейски и регионален аспект е динамична и безусловно оказва влияние върху развитието на Въоръжените сили на Република България. Новите реалности все повече изискват бюджетни ограничения, оптимизиране на системата за отбранителна аквизиция и същевременно стремеж към коопериране при придобиването на необходимите на страната ни отбранителни способности.

Ключови думи: Сигурност, Отбрана, Способности, Аквизиция.

THE CHALLENGES.....

Zhivko LAVCHEV, Assistant professor, Major,
Security and Defense Management Department,
"G.S. Rakovski" National Defense College

Abstract: The political and economic environment in a global, European and regional aspect is dynamic and unconditionally influencing the development of the Armed Forces of the Republic of Bulgaria. The new realities increasingly require budget constraints, optimization of the defense acquisition system and at the same time striving for cooperation in acquiring the necessary defense capabilities of our country

Key words: Security, Defense, Capabilities, Acquisition

Една от основните функции на държавата е да осигурява защита на живота и собствеността на гражданите от вътрешни и външни посегателства. По

тази причина всяка година от консолидирания бюджет се отделят значителни по размер средства за сигурност. Понятието „Сигурност“ „ е едно от най-често употребяваните многозначни съвременни понятия. Сигурността не е самостоятелна наука и дори научна област. Не съществува единна теория на сигурността и поради това нейният предмет не може да бъде определен еднозначно. Област на сигурността може да бъде всеки аспект на международните и вътрешно-национални отношения.“[1], В науката сигурността се изучава в две основни дисциплини – *национална* и *международна*, като делител се явява държавата. *Международната сигурност* може да се определи като набор от мерките, предприети от субектите на международните отношения – държавите и международните организации като (ООН), НАТО, Организацията за сигурност и сътрудничество в Европа (ОССЕ) и други за да се гарантира взаимното оцеляване и безопасност. Тези мерки включват военни действия и дипломатически инструменти като споразумения, договори и конвенции. Международната и националната сигурност са неразривно свързани. Международната сигурност е „националната сигурност“ на световната сцена. Понятието “*национална*

сигурност" се появява най-напред в американската политология. За първи път определението "национална сигурност" е употребено от президента на САЩ Теодор Рузвелт в обръщение към Конгреса, обосновавайки присъединяването на зоната на Панамския канал с интересите на националната сигурност. Национална сигурност е динамично състояние на обществото, при което са защитени териториалната цялост, суверенитетът и конституционно установеният ред на страната, когато са гарантирани демократичното функциониране на институциите, основните права и свободи на гражданите, устойчивото икономическо развитие и благосъстоянието на населението, както и когато страната успешно, защитава националните си интереси и реализира националните си приоритети." [2]

„В научната литература има две популярни схващания за това както включва *„национална сигурност"*: руското разбиране се свежда до състояние на защитеност, сигурност, а американското - до способността на държавата да защитава националните ценности от външни заплахи"[3] и да реализира националните си интереси. В Стратегията за национална сигурност на Република България (СНС) е формулирано, че политиката за национална сигур-

ност е комплекс от взаимно свързани приоритети и секторни политики за сигурност (финансова и икономическа, социална, енергийна, екологична, правосъдие и вътрешен ред, външна, и отбранителна).

Отбранителната политика е политиката на държавата по отношение на създаването, поддържането, развитието и използването на въоръжена сила. Стратегическата цел на отбранителната политика е „защитата и утвърждаването на националните интереси, чрез изграждане, поддържане и използване на адекватни на средата на сигурност отбранителни способности в рамките на единния комплект оперативно съвместими модерни въоръжени сили. Мисиите и задачите на въоръжените сили и приоритетите на отбранителната политика са неразривно свързани с националните интереси.“[4]. „Министерството на отбраната и въоръжените сили осъществяват водещите направления в отбранителната политика под едновременното и комбинирано въздействие на няколко значителни по мащаб и обхват геостратегически, политически и икономически реалности - негативното влияние на световната финансова и икономическа криза, наследството от неефективно управление на отбранителните ресурси и новите условия на средата на сигурност с трудно предвидими и нетрадиционни предизвикателства, рискове и заплахи“ .

В рамките на Отбранителната политика трябва да бъдат разграничени две, макар и тясно свързани направления – *Прилагане на въоръжена сила и Подготовка на въоръжена сила***.** Под прилагане на въоръжена сила следва да се разбира вземането на решение за предприемане на военни действия и провеждането им. Подготовката на въоръжена сила е свързана с отбранителния мениджмънт, чието предназначение е да подготви необходимата за изпълнение на националните цели въоръжена сила, при това на минималната възможна ни цена. За целта в Министерството на отбраната е въведена „Система за управление на развитието на въоръжените сили (СУРВС), осигуряваща ефикасно и ефективно постигане и поддържане на отбранителни способности, произтичащи от националните планиращи документи и плановете за развитие на въоръжените сили в рамките на разполагаемите ресурси, чрез планиране, организиране, изпълнение и контрол на взаимосвързани дейности, изпълнени в строго определена хронология“[5]. СУРВС е регламентирана с постановление на Министерски съвет (ПМС) № 301 от 10.11.2004. обнародвано в държавен вестник (ДВ) бр. 103 от 23.11.2004 г.. Съгласно този документ СУРВС се състои от четири взаимно свързани подсистеми:

- Подсистема за необходимите оперативни способности (СНОС),

предназначена за определяне на изискванията и приоритетите за постигане на необходимите оперативни способности, произтичащи от националните документи и задачи в областта на сигурността и отбраната.

- Интегрирана подсистема за управление на ресурсите за отбрана (ИСУРО), предназначена за определяне на необходимите ресурси за отбрана и кога и как те да бъдат използвани за постигане на дефинираните и подкрепени по приоритети (приоритизирани) НОС.
- Подсистема за отбранителна аквизиция (СОА), предназначена за определяне на оптималния начин, по който следва да бъдат постигнати НОС.
- Подсистема за управление на човешките ресурси.[6]

Или, ако СНОС дава отговор какви способности са необходими и защо, ИСУРО определя целесъобразността дали и кога да се осигурят ресурси за дадена способност, а отговорът на въпроса как да се постигнат тези способности посредством съответствието на технологиите и ресурсната осигуреност, се дава от СОА. Прави впечатление, че тя се явява свързващото звено в зависимостта „ресурси – способности“[7].

От своя страна въпросът за връзката между разходите за отбрана и брутният вътрешен продукт (БВП) на всяка страна на пръв поглед изглежда едностранен и представляващ еднопосочна зависимост. Логиката диктува нарастването на БВП да води до увеличаване на размера на средствата, които държавата може да преразпределя чрез бюджета, съответно нарастване на държавните разходи, което от своя страна да се отрази и на разходите за отбрана. „Отбраната на страната обединява дейностите на държавните органи, институции, организации и гражданите за изграждане и използване на отбранителни способности за разкриване, възпиране, предотвратяване и противодействие на евентуална заплаха за националните интереси. Отбраната е широко обхватна, общодържавна дейност с единно ръководство, планиране, финансово и ресурсно осигуряване. Отбраната на страната се планира, подготвя и осъществява в рамките и с прилагане на механизмите на колективната отбрана на НАТО и общата политика за сигурност и отбрана на ЕС с ефективно използване на националните отбранителни способности, включващи военните и невоенните способности на страната. Изграждането и развитието на отбранителните способности се обвързва със задачите по защитата на националните интереси и с изпълнение на съюзните ангажименти, а приносът към националната сигурност в мирно време се осъществява с използване на вече изградени способности.“[8]

Поддържането на отбранителната способност на страната е задължение

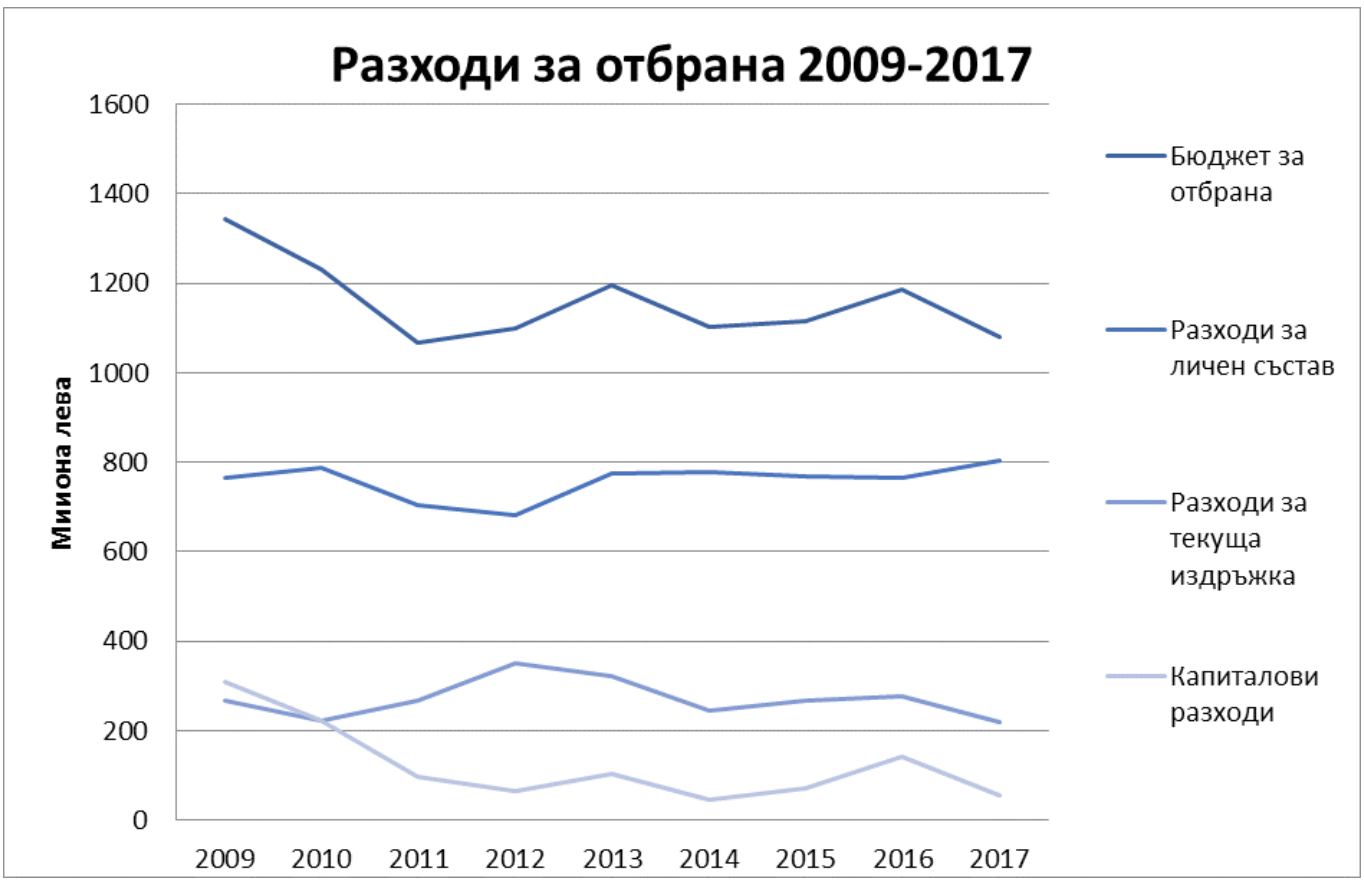
на държавните органи, Въоръжените сили, органите на местното самоуправление и местната администрация, както на гражданите и на юридическите лица. Отбраната се осъществява при ефективно използване на националния отбранителен потенциал, включващ Въоръжените сили и невоенни компоненти. Държавата осигурява необходимите човешки, финансови, материални, административни и инфраструктурни и други ресурси и услуги за изпълнение на задачите по отбраната на страната. Ресурсното осигуряване на отбраната се осъществява чрез планиране, управление и контрол на програмен принцип. В Министерство на отбраната за управление на ресурсите за отбрана, в т.ч. и финансовите се използва програмен подход чрез прилагане на Интегрирана система за управление на ресурсите за отбрана (ИСУРО). Предимствата на ИСУРО са:

- подпомага постигането на дългосрочните национални амбиции, цели и приоритети в сектора на сигурността и отбраната;
- подпомага правилното целеполагане и приоритизиране при планиране на ресурсите за отбрана;
- осигурява ефективно разпределение на ресурсите за отбрана;
- определя ресурсите за отбрана за изграждане/поддържане на необходимите отбранителни способности от ВС;
- осигурява планиране на ресурсите за отбрана по области и елементи на отбранителните способности;
- планирането на ресурсите за отбрана се осъществява чрез отбранителни програми и проекти за модернизация;
- позволява постигане на консенсус в отбранителните програми при планиране на ресурсите за отбрана;
- въвежда показатели (оценители) за оценка на изпълнението на отбранителните програми, съобразени с приетите в НАТО;
- повишава ефективността на гражданския контрол върху изразходване на националните ресурси за отбрана;
- позволява предлагане на алтернативни решения при планиране на ресурсите за отбрана.

Част от дейностите на Министерство на отбраната се финансират извън бюджета на МО чрез - „Програма на САЩ за чуждестранно военно финансиране” (FMF/FMS); „Програма на НАТО за инвестиции в сигурността” (NSIP) и по оперативни програми на ЕС. Чрез реализиране на посочените програми се освобождават финансови средства, които се пренасочват за други приоритетни дейности при изграждане / поддържане на отбранителни способности.

Въпреки редицата негативни предпоставки, част от които не са свързани с България, за 10 години БВП на страната номинално се е увеличил с 50% спрямо 2008 г., достигайки от почти

66 млрд. до почти 100 млрд. лева. Подобно е и състоянието на публичните разходи (Консолидираната фискална програма), които достигат от над 25 млрд. през 2008 г. до почти 35 млрд. лева през 2017 г. В същото време са налице обстоятелства, които сериозно затрудняват пренасочването на ресурс за финансиране на приоритетни политики като цяло и на отбранителната – в частност. Дори да не вземаме предвид периодът преди кризата, когато годишният бюджет на МО надхвърля 1,5 млрд. лева, след 2009 г. се наблюдава относително ясна тенденция за намаляване на общите разходи за отбрана. Но в случая не това е най-важното. От по-голямо значение за бъдещето развитие на отбранителните способности е вътрешното разпределение на разходите за отбрана. Посочените в графиката равнища на разходите в трите основни категории обясняват тревожните констатации по отношение на боеспособността на въоръжените сили:



В Министерството на отбраната „ролята на СОА е по най-ефективния начин да се придобият отбранителни продукти, необходими за изпълнението на мисиите и да осигури дългосрочната им поддръжка при спазване

на изискванията и приоритетите посочени е Подсистемата за НОС и утвърдените ресурси в ИСУРО“[9]. Или „в рамките на СОА се осъществява планирането на материалното осигуряване на необходимите и интегрирането на новопридобитите способности на ВС, като израз на фазите на жизнения цикъл на отбранителните продукти и военната инфраструктура“[10]. Нейният комплексен характер и широкият и мащаб предопределят сложността на структурата, процесите и взаимовръзките в СОА. Тя определя начина, по който следва да бъдат постигнати способностите в рамките на определени срокове и налични ресурси. Чрез нея въоръжените сили придобиват, експлоатират и поддържат необходимите им отбранителни продукти в интерес на бойната подготовка на въоръжените сили, участието им в национални и международни учения , съюзнически и коалиционни операции и мисии, подпомагане на населението в случай на аварии, стихии и природни бедствия и др. СОА обхваща и трите нива на управление на отбраната и въоръжените сили и допринася в значителна степен за изпълнението на ангажиментите на Република България към НАТО и Европейския съюз, поети под формата на Цели на способности и декларирани формирования за участие в пълния спектър на операции на двата съюза. СОА се състои от множество процеси, които трябва да бъдат изпълнени за придобиване на необходимото въоръжение, техника и системи за нуждите на Министерството на отбраната. Последващия анализ на СОА е извършен по метода SWOT, като предмет са вътрешните и външните фактори, които влияят на системата.

Силни страни:

Системата за отбранителна аквизиция функционира повече от 15 години и чрез изградена за това структура, дефинирани процеси, практики и функции, които се изпълняват профилирано и по компетентност от различни структурни единици във вътрешната среда. Има ясно определени отговорности, функционира чрез щатни и нещатно органи и има възможност за осъществяване на лесен и ефективен контрол от страна на ръководството на министерството. Разполага с добра база документи регламентиращи изпълнението на процесите и взаимовръзките в нея. Организирането на процедурите по обществени поръчки е на добро ниво. Постоянно се оптимизира процеса свързан с кодификацията на материални средства.

Слаби страни

Налице е нужда от актуализиране или пълно премахване на вътрешноведомствени документи, както и разработване на нови такива, така че

адекватно да бъдат регламентирани всички аспекти на отбранителната аквизиция. Честите структурни промени, недостига на кадри и загубата на приемственост се отразяват изключително негативно на системата. Липсва единна електронна система за електронно управление на процесите по заявяване, възлагане, изпълнение и приключване на договорите и анализ на резултатите, както и усложняване на каналите за комуникация, които са предпоставка за забавяне на изпълнението на определени дейности от процесите. Налице са условия за нарушаване на интегритета при управлението на системата и разкъсване на взаимовръзките между отделни звена от нея, както вътрешни за МО, така и външни. Липсва централизиране на процесите по управление на жизнения цикъл на отбранителни продукти на стратегическо ниво Всеки второстепенен разпоредител с бюджетни средства сам решава какви са му приоритетите, какво и колко да придобие. Това е причината в Българската армия да има десетки различни видове техника, която се поддържа по различен начин. Това се отразява и върху желанието на евентуалните доставчици на отбранителни продукти да участват в обществени поръчки – нищожно малките заявени количества. В същото време и други видове въоръжени сили и структури на подчинение на Министерството на отбраната имат нужда от същите отбранителни продукти, но за съответната финансова година са определили друг приоритет и нямат планирани финансови средства за тях. В много случай, също така, се забавя стартирането на процедура по възлагане на обществена поръчка поради липса на актуална техническа спацификация/ тактико-техническо задание (ТС/ТТЗ) свързана с искане на заявителите за доставка или услуга по дадена позиция от единен финансов план за материално-техническо осигуряване (ЕФП за МТО). Изискванията, дефинирани в заявките за разработване на ТС често не съответстват на наличните продукти на пазара или въвеждат ограничителни условия, които намаляват броя на потенциалните изпълнители (доставчици) и като резултат водят до висока цена на придобиване. Получаването на заявки за един и същи продукт с различни изисквания от отделни заявители, води до изготвяне на няколко ТС/ТТЗ и организиране на различни процедури за един и същ продукт. В следствие заявените количества не предизвикват интерес за потенциални доставчици. Честите изменения в ЕФП за МТО водят до необходимост заявените ТС/ТТЗ да бъдат изготвени в критично кратки срокове, което не позволява да бъде направено необходимото проучване за продукта на пазара, както и оценка на въздействието на околната среда и оценка на всич-

ки съпътстващи разходи по време на жизнения цикъл на изделието. Липсва достатъчно ефективен анализ и контрол на резултата от придобиването на отбранителни продукти по отношение на придобитите способности и влиянието им върху системата от отбранителни способности. Изпълняват се договори по проекти, които не са включени в портфолиото на Министерството на отбраната. Решават се въпроси за развитие (модернизация) на системи чрез рамкови договори. Затруднява се проследяването на вложения финансов ресурс за поддръжка, експлоатация и модернизация на отбранителни продукти (системи, съоръжения и др.). Непълните, неточни и неясни искания, често за един и същ продукт от различни заявители, през цялата финансова година водят до откриване и възлагане на финансово неосигурена обществена поръчка. Тежки са процедурите по съгласуване на документация и прекалено тромавите и бюрократични вътрешни правила за управление на цикъла на обществени поръчки водят до разходване на неоправдано голям ресурс от експерти по изготвяне на различни видове документации.

Възможности, които представя външната среда

На първо място използването на чужд опит по отношение на изграждането и функционирането на СОА и процесите в нея. Използване на възможностите на Агенциите на НАТО (NSPA[1] и NCIA[2]) и Европейската отбранителна агенция. Програмата за чуждостранно военно сътрудничество[11] на САЩ – FMF/FMS и Програмата на НАТО за инвестиции в сигурността – NSIP, както и включване в Постоянното структурирано сътрудничество на Европейския съюз. Засилване на взаимодействието и връзките с другите ведомства, Българската отбранително-технологична база (БОТИБ), използване на външна експертиза в изготвяне на по-ефективни и гъвкави правила за провеждане на обществени поръчки и др.

Заплахи от външната среда

Динамично развиващата се международна обстановка и непрекъсната пропагандна война в интернет пространството са едни от новите заплахи на външната среда влияеща на националната сигурност. Освен тях на системата влияят неосигурено финансиране и/или липса на дългосрочно планиране на финансирането. Недостатъчни дейности по НИРД в областта на сигурността и отбраната в общата научна област на страната, както и липса на познания свързани със системите за отбранителна аквизиция на други страни.

1 NATO Support and Procurement Agency
2 NATO Communications and Information Agency

На база на направения анализ можем да изведем на преден план следните предложения: необходимо е да се проучат чуждестранните практики и опит в областта; необходимо е усъвършенстване на вътрешните за СОА процеси на функциониране за осигуряване на по-висока ефективност и резултатност[12]; необходимо е създаване на платформа за електронно управление на процесите, интегриране на съществуващи такива и автоматизиране на дейностите от СОА; необходимо е оптимизиране на процеса на съгласуване чрез осигуряване на процедура за самостоятелно придвижване на документи между съгласуващите структури; необходимо е провеждане на конкурси за попълване на незаетите работни места и организиране на специални курсове за обучение на личния състав, осъществяващ процесите в СОА[13]; необходимо е привързване на действащите договори, свързани с модернизация и развитие, към съответен проект (разработване на проектна документация) и разработване на програми за управление на жизнения цикъл на отбранителни продукти (проекти за придобиване, проекти за модернизация, планове за експлоатация и поддръжка); необходим е задълбочен анализ при обработка и обобщаване на получените в Дирекция "Отбранителна аквизиция" заявки за изработване на ТС/ТТЗ, както и на получените Искания за доставка/услуга с цел подобряване на планирането и избягване на ангажирането на ресурс за организиране и провеждане на няколко обществени поръчки с еднакъв предмет; необходимо е облекчаване на Вътрешните правила за управление цикъла на обществени поръчки чрез опростяване на вътрешните процедури; необходимо е урегулиране на срока за постъпване на искания в Дирекция "Отбранителна аквизиция" с цел спазване на законоустановените срокове съгласно ЗОП и увеличаване на възможността за придобиване на определена способност.

(Endnotes)

1 Симеонов, Т. Правна уредба на мениджмънта на сигурността и отбраната, София, 2014 г.

2 Димов, Г. Същност и съдържание на националната военна стратегия, София, 2008 г..

3 Симеонов, Т. Правна уредба на мениджмънта на сигурността и отбраната, София, 2014 г.

4 Програма за развитие на отбранителните способности, 2016.

5 Вълков, И. Трансформация на отбрнаителните способности, 2010 г..

6 Иванов, Г. Управление на личен състав във военни формирования, Диомира, София, ISBN 978-954-2977-21-6 2015, с. 91.

7 Димитрова, С. Управление на

ресурсите за отбрана в сектора сигурност, В.Т. 2011, с.146
8 Симеонов, Т. Правна уредба на мениджмънта на сигурността и отбраната, София, 2014 г.
9 Алашки, М. Системата за отбранителна аквизиция на Република България – възможност за усъвършенстване, 2016
10 Димитрова, С. Отбранителна аквизиция като елемент на управлението на ресурсите за отбрана
11 Лазаров, В., Новите реалности иразузнаване с хора, Издателство „Изток-запад“, 2012, ISBN 619152051-4, с. 169
12 Лазаров, В., Матрични решения за националната сигурност, Издателство „Изток-запад“, 2012, ISBN 619152096-4, с. 162.
13 Иванов, Г., Подбор, подготовка, оценка и развитие на служители във военната организация, гр. София, Издателство „ДиоМира“, ISBN 978-954-2977-49-0, 2018, с. 16

Източници на несигурност в Европа, влияещи върху средата за сигурност – причини, последствия и възможни решения

Автор: Майор Валентин Иванов Георгиев
докторант, редовна форма на обучение в катедра „Съвместни операции и планиране“,
факултет „Национална сигурност и отбрана“

SOURCES OF INSURANCE IN EUROPE INFLUENCE ON SECURITY ENVIRONMENT - CAUSES, CONSEQUENCES AND POSSIBLE SOLUTIONS.

Резюме: *Настоящият доклад е основан на въздействието на различните видове източници на несигурност и влиянието им върху средата за сигурност. Ще бъдат разгледани факторите за възникване им и тяхното влияние върху средата за сигурност в държавите от Европа, в това число и в Република България. Настоящият доклад ще обхване миграцията, тероризмът и хибридните заплахи, както и влиянието им върху средата за сигурност. Как всеобхватния подход би способствал за намаляване на въздействието на източниците на несигурност върху средата за сигурност в Европа? И какви мерки е необходимо да бъдат набелязани за да се повиши ефективността на предприетите мерки срещу източниците на несигурност.*

Ключови думи: *Всеобхватен подход, източници на несигурност, среда за сигурност, ООН, НАТО, Европейски съюз, миграция, тероризъм, хибридни заплахи*

Abstract: *This article on the report is based on the return of types of sources of uncertainty and impact on the security environment. This concerns the security environment of Europe, including the Republic of Bulgaria. Tips for overcoming problems. In this report, the report covers migration, terrorism and hybrid threats, as well as the impact on the security environment. Whatever is the first efforts to introduce information and possibly introduce the economy in Europe. How*

a comprehensive approach would help reduce the impact of sources of insecurity on the security environment in Europe? And what measures need to be targeted to increase the effectiveness of the measures taken against sources of uncertainty.

***Keywords**: Comprehensive approach, sources of insecurity, security environment, UN, NATO, European Union, migration, terrorism, hybrid threats*

Съвременната среда за сигурност се характеризира със своята сложност, непредвидимост и непостоянност. За да може една държава или международна организация да отговори адекватно на източниците на несигурност, влияещи върху средата за сигурност, е необходимо да бъде извършван постоянен мониторинг на заплахите, влияещи върху сигурността. От една страна е необходимо да бъде извършен анализ на всяка една заплаха и нейният произход. Какви са първопричините за възникването ѝ назад във времето като се обхванат исторически, политически, военни, социални, културни и икономически аспекти. А от друга да се наблюдава и опознава влиянието на заплахата върху средата за сигурност. На базата на това може и трябва да се набележат превантивни мерки за неутрализиране на заплахата или минимизиране на въздействието ѝ върху средата за сигурност. Този процес е нескончаем, постоянен, защото както знаем, изследването и анализирането на средата за сигурност не може да бъде застинал процес.[1]

Настоящата статия има за цел да обхване част от източниците на несигурност, влияещи върху средата за сигур-

ност в Европа и Република България. Поради различните източници на несигурност, ще бъдат разгледани влиянието на миграцията, тероризмът и хибридните заплахи върху средата за сигурност в Европа и Република България.

Миграцията към Европа.

Въоръжените конфликти в Близкия изток, Азия, Африка и икономическите и хуманитарни кризи в следствие на преминалите или продължаващи конфликти са една от причините за огромните бежански потоци към Европа. Пред хората, които са принудени да мигрират, стои реална заплаха за живота им и те търсят закрила в друга държава. Според конвенцията за бежанците[2], защитата се предоставя на хора, които бягат от родните си страни и не могат да се върнат поради основателен страх от преследване или риск за живата им или от сериозно увреждане. Инициативата за подпомагане на бежанците се подкрепя основно от Върховния комисариат за бежанците към ООН и на базата на което държавите от ЕС и самата организация имат правно и морално задължение да защитават нуждаещите се. Държавите-членки на ЕС имат задължение, свързано с разглеждането на молбите за убежище и за вземането на решение за това кой ще получи закрила. Непрекъснато се работи за гарантиране на предприемането на адекватни мерки за закрила на децата. Това се превръща във все по-неотложен въпрос, тъй като броят на децата в миграция, особено тези, които са без придружител, нараства. Тези деца са изключително уязвими и изискват специално внимание и грижи.

Но, не всеки, който идва в Европа, се нуждае от защита. Много хора напускат домовете си в опит **да подобрят** живота си. Тези хора често се наричат икономически мигранти и ако те нямат легитимно право на защита, националните правителства имат задължението да гарантират, че ще ги върнат (или доброволно, или с помощта на принудителни мерки) в родната им страна, или друга страна, през която са преминали. Вследствие на неконтролираната и нерегламентирана миграция, хиляди хора са загинали в моретата и океаните, опитвайки се да стигнат до желана страна от ЕС. Много голяма част от бежанците и мигрантите плащат на организирани престъпници и контрабандисти на хора, за да ги прехвърлят през границите.

Осигуряването на храна, вода и подслон на хората се явява огромна тежест върху ресурсите на някои страни от ЕС. Това особено важи за Гърция и Италия, където пристигат основната част от бежанците в Европа. В така наречената Шенгенска зона, хората могат да се движат свободно без контрол на вътрешните граници, но притокът на мигранти принуждава някои страни от ЕС да въведат временни проверки на границите си с други държави от Шенген.

Миграционната криза достига своя пик през 2015 г. и беше показателна с факта, че държавите в Европа не бяха готови както за осигуряването на сигурността в страните членки, така и със справянето с бежанския поток по външните граници на Съюза. Политическата криза около миграцията на бежанци разкри фундаментални разделения по отношение на начина, по който държавите в Европа възприемат същността на термина „сигурност". На моменти липсваше консенсус и ясни намерения какви действия е необходимо да бъдат предприети за да бъде решен проблема.

Част от държавите в ЕС бяха за изграждане на огради по границите си, като по този начин се насочи бежанския поток към граничните пунктове в това число и Република България, за да се извършва контрол на потока. Друга част от държавите в Европа бяха за пълно затваряне на границите си. И именно докато траеше този процес на вземане на решение какви действия е необходимо да бъдат взети в Европа, върхът на мигрантската криза е през 2015 г. и 2016 г., като на територията на Европа навлизат 2 583 700[3] мигранти. Този поток оказва не само икономическа тежест върху държавите в Европа, но се явява и един от основните източници на несигурност, поради факта, че няма как да се знае колко от тях са членове или поддръжници на терористичните организации.

От своя страна бежанския поток се оказва едно голямо предизвикателство, стоящо пред външната и вътрешна политика на правителството на Република България. Поради географското ни разположение, границите на Република България са външни за Европейския съюз (ЕС) и НАТО, което доведе до значително повишаване на миграционните, криминални и контрабандни потоци през територията ни. И от друга страна близостта на страната ни до „горещите" точки на конфликтите предполага засилване на рисковете и заплахите пред сферата на сигурността.

В тази връзка, е необходимо международните организации (ООН, ЕС и НАТО) да създадат условия за умиротворяване на Близкия изток и условия за икономическо възстановяване. Като друга мярка е необходимо активно участие на Република България във формирането на единна миграционна политика за бежанците, в която България като външна граница да не бъде буферна зона. Защото това от своя страна крие много рискове и заплахи пред сферата на сигурността в България.

Миграцията и тероризмът

Представлява ли миграцията реална заплаха за Република България и Европа? Миграцията, по своята същност, е търсене на закрила на застрашени лица с опасност за живота си или тежки увреждания в собствената си държава, и защитени от „Конвенцията за бежанците" на ООН. Но на практика,

освен лицата нуждаещи се от закрила е възможно да има и такива лица с не дотам „мигрантски“ намерения. И в този смисъл миграцията може да бъде начин за инфилтриране на терористи и престъпници. От една страна има много малко доказателства, от която и да е страна по света, за концентрацията на терористи, потенциални такива или престъпници сред мигрантския поток. Но от друга страна, налагането на мигранти с етикети без обосновка рискува допълнително да противодейства на обществените нагласи към тях. Не бива да пренебрегваме и факта, че съсредоточаването само върху тези крайности крие риск за отклоняване на вниманието от обстоятелства, при които миграцията действително може да представлява заплаха за националната сигурност.

Например, незаконната миграция може законно да се разглежда като подкопаване на държавния суверенитет, тъй като всяка държава има право да контролира кой преминава границите ѝ и кой се намира на нейна територия. Все пак неспособността за контрол и управление на миграцията рискува да подкопае общественото доверие в правителствената политика по отношение на мигрантите. Разрастващата се контрабанда на мигранти и индустрии за трафик на хора могат да представляват истинска заплаха за закона и реда, особено когато са свързани с организираната престъпност и се пресичат с движението на незаконни стоки, включително оръжия и наркотици. В този случай, не мигрантите, а онези, които се възползват от тях, нарушават законите.

Пристигането на голям брой мигранти, особено от много различен социален или културен произход, отколкото приемащите общности, също може да представлява сериозно предизвикателство за социалното сближаване. Това може да има практически последици за държавите, например по отношение на разпределението на ресурсите, както и повече концептуални последици по отношение на моделите на интеграция и националната идентичност. Мигрантите могат да се конкурират с местните жители на пазара на труда, особено по време на рецесия, икономически спад и по този начин да станат магнити за негодувание. Когато голям брой хора се заселват в ограничена зона за дълъг период от време, какъвто е случаят с някои бежански и лагери за вътрешно разселени лица, те могат да имат пагубен ефект върху местната околна и социално-икономическа среда.

Голяма част от мигрантите нямат документи или влизат нелегално, което от своя страна представлява възможност за навлизане на „недоброжелателни“ лица с евентуални терористични намерения, в следствие на което терористичните атаки не подминаха и Европа. Този вид заплаха е една от основните за средата за сигурност на държавите в Европа и света. На базата

на публикуван анализ на EUROPOL[4] е представена графика показана на фигура 1, от където е видно, че въпреки многобройните арестувани евентуални извършители, терористичните атаки се увеличават всяка година.

Фигура 1 – графика на извършените арести, извършените терористични атаки в Европа и загинали граждани.

Извършените терористични атаки подчертаха недостатъците в националните рамки за вътрешна сигурност на държавите и така необходимото споделяне на информация между държавите и невъзможността в някои случай да се обхванат всички сухопътни граници с което да се гарантира граничния контрол. Като за някой държави от Европа, наблюдението на сухопътните граници не може да се обхване поради релефни особености или недостатъчен на брой личен състав за охрана на границите.

Това от своя страна представлява заплаха за сигурността както в България, така и в Европейския съюз поради възможността да са се инфилтрирали лица с недобросъвестни намерения срещу гражданите на Европейския съюз. Затова е необходимо въвеждане на нови механизми за борбата с тероризма: Повишаване на съществуващата поддръжка за мониторинг и противодействие на радикализацията в Европа и споделяне на информацията с което ще се постигне по-добър обхват на разпространението ѝ и условия за по-добро противодействие; И на последно място, но не и по важност – едновременното използване на всички инструменти за въз-

действие, което би довело до повишаване на ефективността на усилията в борбата срещу тероризма.

Хибридна война

Поради факта, че термина „хибридна война“ е сравнително нов, ще разгледам неговата същност и различните схващания за същността му. Според някой автори, „хибридната война“ се разглежда като комбинация от постоянни и непостоянни форми на военни действия[5].

По своята същност терминът „хибрид“ произхожда от биологията, където означава животно или растение, получено в резултат на съвместяване на генетично отделни индивиди[6]. В руската езикова научна литература[7] тълкуването - хибридна война е много по-просторно. Сферата на хибридната конфронтация разчита на всички основни сфери на социална активност. Някой руски автори дават изключително описателни определения, и подробности чрез изброяване на признаци на хибридна война в различни обществени сегменти от живота. Според професор Наталия Комлева[8], хибридната война е само геополитическо явление, което не е напълно определено в други изследвания. Основните геополитически пространства, представени в публикацията[9] й, обхващат: 1) географското, 2) икономическото, 3) идеологическото - информационно пространство. Като разгледаните начини за водене на хибридна война се различават в зависимост от спецификите на всеки тип пространство.

1. Основните начини за провеждане на хибридна война в географско пространство са разгледани[10] като:

Местни „традиционни“ войни в ресурсните региони на целевата държава агресията, участието на страната в поредица от “интензивни конфликти” по периметъра на нейните граници;

„Цветни революции“ , т.е. състояние на преврат в целевата страна набелязана за агресията и/или в нейните геополитически държави-съюзници;

Насърчаване на сепаратизма в страната - обект на агресия.

2. Основните начини за провеждане на хибридна война в икономическото пространство, са разгледани[11] като:

Санкции срещу отделни сектори на икономиката на страната - обект на агресия, включително затварянето на международните пазари за санкционираната страна и блокиране на достъпа до определени технологии;

Санкции срещу всички сектори на икономиката на страната - обект на агресия в съвкупност (икономическа блокада);

Санкции срещу ключов персонал, определящ съдържанието и хода на икономическите процеси в страната - обект на агресия.

Като пример можем да посочим Русия, която в момента е подложена на икономически санкции от САЩ, ЕС, Австралия, Канада, Япония и някои други страни, началото на които се постави през 2014 г. след присъединя-

ването на Крим към Русия.

3. Основните начини за провеждане на хибридна война в информационно-идеологически пространство, са разгледани[12] като:

заместване на традиционните ценности и идеологически схващания на дадено общество с ценности и идеологически схващания на друго общество;

фалшифициране на тълкуването на историята на страната-обект на агресия;

Според схващанията на НАТО термина Хибридна война[13] е разгледан, като: „Използване на комбинация от конвенционални и неконвенционални средства от враждебни държавни, които могат същевременно да избягват отговорността за своите действия. Една от основните характеристики на хибридната война е привличането на всички инструменти на властта, като се ограничава конфликтът под прага на конвенционалната война, което усложнява навременното и ефективно използване на твърдите механизми за колективна защита. Хибридната война може да включва използването на пълномощни, законни средства и информационна война с цел да се създаде неяснота и несигурност“

По своята същност термина „хибридна война“ е сравнително нов, като такъв. Използването му като инструмент цели да създаде благоприятни условия за достигане на желани политически условия, такива от които агресорът (било то държава или участник) да извлече ползи и облаги. Първоначалните въздействия върху набелязаната цел (държава) е скрито и понякога трудно забележимо. Именно това прави тези заплахи опасни, поради факта, че чрез хибридните войни се цели да се въздейства върху дадена област от държавното управление или върху държавата като цяло[14]. *Хибридната война генерира сложни заплахи, които се променят по форма и външен вид. Същността ѝ се състои от интегрирано използване на конвенционални и неконвенционални средства, както открити, така и скрити, включително (пара) военни и цивилни участници, за да се създаде неяснота и да се насочат уязвимостите на противника за постигане на геополитически и стратегически цели. Измамата и манипулираните информационни операции имат важна роля в хибридната война и* „Съвременната информационна война може да се води постоянно, анонимно и незабележимо във всяка точка на информационното пространство, включително и на чужда територия. Обект на въздействие са културното пространство на противника и неговото съзнание, докато той дълго време може въобще да не осъзнава, че е цел на информационно въздействие или дори на външно управление. Всичко това осигурява значителна ефективност на методите за въздействие при минимални загуби и разходи за агресора, което му поз-

волява да запази и поддържа образ на миролюбива и цивилизована държава“[15]

Според доклад от срещата на върха в Брюксел на НАТО на 12 юли 2018 г. - Русия оспорва Евроатлантическата сигурност и стабилност чрез хибридни действия, включително опити за намеса в изборните процеси и суверенитета на държави от Алианса, и като примери са посочени случаите в Черна гора, широко разпространени кампании за дезинформация и злонамерени кибер-дейности. Според представения доклад[16]: държави членки на НАТО и ЕС, са: „Подложени на нарастващо предизвикателство както от държавни, така и от недържавни участници, които използват хибридни дейности, които имат за цел да създадат неяснота и да замъглят границите между мира, кризата и конфликта. Въпреки, че основната отговорност за отговора на хибридната заплаха има потърпевшата държава, НАТО е готов, по решение на Съвета, да окаже съдействие на съюзник на всеки етап от хибридната кампания. В случаите на хибридна война, Съветът може да реши да се позове на член 5 от Вашингтонския договор, както в случай на въоръжено нападение. Повишаваме устойчивостта си, подобряваме осведомеността си за ситуацията и засилваме нашата възпираща и отбранителна позиция. Ние също така разширяваме инструментите, с които разполагаме, за справяне с враждебни хибридни дейности. Съобщаваме за създаването на екипи за противоположна хибридна поддръжка, които предоставят специализирана, целенасочена помощ на съюзниците, по тяхно искане, в подготовката и реагирането на хибридни дейности. Ние ще продължим да подкрепяме нашите партньори, тъй като те укрепват тяхната устойчивост пред хибридните предизвикателства.“

Въпреки основната отговорност за отговора на хибридната заплаха да е на потърпевшата държава, НАТО има готовност, по решение на Съвета, да окаже съдействие на съюзник на всеки етап от хибридната кампания. Като в случай на хибридна война, Съветът може да реши да се позове на член 5 от Вашингтонския договор, както в случай на въоръжено нападение.

На срещата на върха в Брюксел на НАТО на 12 юли 2018 г. е взета инициатива[17] за сили с висока степен на готовност, т. нар. Инициатива 4х30. В рамките на общите сили, съюзниците трябва да имат на разположение 30 кораба, 30 батальона, 30 ескадрили, с готовност 30 дни или по-малко. Целта е те да бъдат организирани и обучени като елементи на по-големи бойни формирования в подкрепа на цялостното възпиране и отбранителна позиция на НАТО до 2020 година. Инициативата за готовност на НАТО допълнително ще засили способността на Алианса за бързо реагиране, или за укрепване на съюзниците в подкрепа на възпиране или колективна отбрана, включител-

но за високоинтензивни бойни действия, или за бърза военна интервенция при криза.

Разбира се, няма как НАТО като чисто военна структура да разреши кризите и да отговори на заплахите, само с военна сила. Необходимо е да е налице адекватно подготвен персонал за координация и взаимодействие с гражданските участници в такива ситуации. **Координацията и сътрудничеството между военните и гражданските участници се явява и ключов момент при прилагането на всеобхватния подход при разрешаването на кризи**. А именно чрез „обучение на персонал, специалисти и експерти по гражданско-военно сътрудничество и гражданско-военни взаимоотношения ще е реално предизвикателство, но именно така ще се подобри ефективността от дейностите и задачите в различни и непривични досега домейни и области от средата на сигурност“[18].

Според схващанията на Европейския съюз термина „хибридна война“[19] е разгледан, като: „Хибридни заплахи съчетаващи в себе си конвенционални и неконвенционални, военни и невоенни дейности, които могат да бъдат използвани координирано от държавни или недържавни участници за постигане на конкретни политически цели. Хибридните кампании са многоизмерими, съчетаващи принудителни и подривни мерки, като използват както конвенционални, така и нетрадиционни инструменти и тактики. Те са проектирани да бъдат трудни за откриване. Тези заплахи са насочени към критични уязвимости и се стремят да създадат объркване, за да възпрепятстват бързото и ефективно вземане на решения.“

Хибридните заплахи могат да варират от кибератаки до критични информационни системи, чрез прекъсване на критични услуги като енергийни доставки или финансови услуги, до подкопаване на общественото доверие в държавните институции или към задълбочаване на социалните различия. Според ЕС, хибридни заплахи са и химичните, биологичните, радиологичните и ядрените заплахи, доставяни чрез неконвенционални средства, попадащи в тази категория заради потенциалния мащаб на щетите, които могат да причинят.

Имайки в предвид обхвата и същността на изложените до момента схващания за хибридните войни, е видно че няма как една организация или държава самостоятелно да се защити и справи самостоятелно с всички аспекти на „хибридна война“. За справянето с този вид заплаха е необходимо прилагането на всеобхватния подход, съчетаващ в себе си всички инструменти на мощта и способности на дадена държава или международни организации.

Сътрудничеството между ЕС и НАТО за противодействие на хибридните заплахи е една от основните насоки за

взаимно допълване на инструментите на мощта на двете международни организации, и чрез които инструменти би следвало да се противодейства на заплахите на средата за сигурност. В първия доклад[20], свързан с напредъка по изпълнението на общия набор от предложения между НАТО и ЕС, десет от четиридесет и две предложения са свързани с борбата срещу хибридните заплахи. Двете международни организации, заедно с държавите-членки и съюзниците, с подписването на декларацията за изпълнението на общия набор от предложения имат амбицията да допринесат и да участват в дейностите на Европейския център за противодействие на хибридните заплахи (ЕЦПХЗ), създаден в Хелзинки[21]. Тук ключов момент се оказва по-добрата възможност за осведоменост за ситуацията, която се явява и от решаващо значение за навременното и ефективно противодействие на хибридните заплахи. Създаването на ЕЦПХЗ на ЕС и взаимодействието му с новосъздадения център за анализ на хибридните заплахи на НАТО ще помогне за изграждането на обща картина на ситуацията в Европа. Това ще способства за превантивни, адекватни и най-вече ефективни мерки срещу заплахите за средата за сигурност в Европа.

Заключение

Разгледаните източници на несигурност са такива заплахи за сигурността на членовете на международните организации и държавите в Европа, че нито една страна няма капацитета да се справи самостоятелно, с който и да е от разгледаните източници на несигурност. Именно това налага изискването да се прилага всеобхватния подход за превенция и минимизиране на надвисналите заплахи над Европа и Република България, като част от нея.

Необходимо е всички участници прилагащи всеобхватния подход да разберат предизвикателството не само от собствените си гледни точки, но и от тези на другите основни участници. Много възприемани заплахи (тероризъм, организирана престъпност, насилствен екстремизъм) са симптоми или последици от основни причини (бедност, етнически конфликти), които не са в правомощията на повечето организации. Именно затова не е достатъчно да се разчита само и единствено на международните организации, а е необходимо да се създадат необходими механизми за противодействие на заплахите **вътре в самите държави.** Като едновременно тези действия са съгласувани с международните организации и с останалите държави. Координацията и взаимодействието от една страна между държавите и от друга страна между

международните организации, ще способства за повишаването на ефективността на действията срещу надвисналите заплахи над Европа и наличието на способности за адекватен отговор срещу тях.

(Endnotes)

1 *Стойчев, Стоян, „Изследване способностите на НАТО и ЕС за отговор и управление на кризи“, Военна академия, 2015, монография, ISBN 978–954–9348–62–0, стр. 17*

2 *Ключов правен документ на ООН подписан през 1951, върху който се гради днешната международна закрила на бежанците. Конвенцията дефинира кой е бежанец и какви видове правна закрила, друга помощ и социални права следва да получат бежанците в държавите, които са се присъединили към документа. https://www.unhcr.org/protection/basic/3b66c2aa10/convention-protocol-relating-status-refugees.html?query=1951 %20convention%20text – посетено на 02.02.2019 г. в 21.00 часа*

3 *Количеството мигранти са на базата на публикация на Eurostat statistic explained, публикувана на https://ec.europa.eu/eurostat/statistics-explained/index.php/Asylum_statistics, посетено на 23.1.2019 г.*

4 *http://www.europarl.europa.eu/news/en/headlines/security/20180703STO07125/terrorism-in-the-eu-terror-attacks-deaths-and-arrests - посетено на 23.1.2019 г.*

5 *Frank G. Hoffman. Conflict in the 21-th Century: the Rise of Hybrid Wars. Arlington,VA: Potomac Institute for Policy Studies, December 2007 [Electronic resource]. URL: www.potomacinstitute.org/images/stories/ publications/potomac_hybridwar_0108.pdf – посетено на 03.02.2018 г.*

6 *http://rechnik.info/%D1%85%D0%B8%D0%B1%D1%80%D0%B8%D0%B4 – посетено на 03.02.2018 г. в 19.40 ч.*

7 *Гибридные войны» в хаотизирующемся мире XXI века / под ред. П. А. Цыганкова. М., 2015 – посетено на 03.02.2018 г.*

8 *Руски професор доктор на политическите науки.*

9 *Комлева, Наталия, Хибридната война – същност и специфика, 2017 г.,*

10 *Пак там*

11 *Пак там*

12 *Пак там*

13 *Framework for future Alliance operations, 2018 -https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf, посетен на 02.022019 г. в 15.40 ч.*

14 *Димов, Петко Основни характеристики на операционната среда и алгоритъм на хибридната война, сп. Военен журнал „ВА Г.С. Раковски“ София, 2016 г. бр.1 стр.86-96*

15 *Желев, Живко, „Информационни операции и информационно въздействие“, Военна академия, 2018, мо-*

нография, ISBN 978-619-7478-01-03, стр.36

16 *https://www.nato.int/cps/en/natohq/official_texts_156624.htm - посетено на 02.02.2019*

17 *Пак там*

18 *Кисьов, Милен, „Новите предизвикателства и подхода на функцията и способността „гражданско-военно сътрудничество“, списание „Българска Наука“, https://nauka.bg/*

19 *https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en, посетен на 02.022019 г. в 12.30 ч.*

20 *Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils from 6 December 2016*

21 *Създаването на Европейския център за противодействие на хибридните заплахи има за цел да се събира информация и разузнавателна информация с цел да се информират институциите в ЕС и останалите държави членки.*

сп. “Българска Наука”, брой 116

Предизвикателства и перспективи за набирането на военнослужещи за нуждите на въоръжените сили

Автор: Полк. доц. д-р инж. Галин Иванов

Полковник доцент доктор инж. ГАЛИН ИВАНОВ е преподавател във Факултет „Национална сигурност и отбрана“ на Военна академия „Г. С. Раковски“, София и хоноруван преподавател в Правно-историческия факултет на Югозападния университет „Неофит Рилски“, Благоевград. Хабилитиран в професионално направление „Сигурност и отбрана“. Автор е на три книги и множество научни статии и доклади. Офицер от кариерата с доказан практически опит в сферата на националната сигурност. Експерт в областта на мениджмънта на човешките ресурси, подбора, обучението, кариерното развитие и административното осигуряване в сектора за национална сигурност.

Участва в множество научноизследователски проекти и колективи за разработване на стратегически и доктринални документи в областта на сигурността и отбраната. Член е на съюза на учените в България.

Анотация: *Статията представя накратко действащия модел за набиране на военнослужещи за нуждите на въоръжените сили. Проучени са проблематичните направления в реализацията на набирането на човешки ресурси за Въоръжените сили на Република България. Очертани са предизвикателства и перспективи за набирането на военнослужещи.*

Ключови думи: *набиране на човешки ресурси, кариерно развитие, човешки ресурси, човешки фактори, управление на човешките ресурси, организационно управление, планиране на човешките ресурси.*

CHALLENGES AND PERSPECTIVES FOR COLLECTIONOF MISCELLANEOUS FOR THE NEEDS OF ARMED FORCES

Galin IVANOV, PhD, Associate Professor, Colonel,
Security and Defense Management Department,
National Defence College "G. S. Rakovski"

Annotation: *The article briefly presents the current model for recruiting military personnel for the needs of the armed forces. The problematic directions in the realization of the human resources recruitment for the Armed Forces of the Republic of Bulgaria were studied. Challenges and prospects for military recruiting are outlined.*

Key words: *human resources recruitment, career development, human resources, human factors, human resources management, organizational management, human resource planning.*

Човешките ресурси са най-важният елемент на отбранителните способности и основен капитал на въоръжените сили. Този потенциал следва да се управлява разумно и изисква да се създават условия за неговата пълноценна реализация. Посредством управлението на човешките ресурси се осъществява политиката на Министерството на отбраната за комплектуване на Въоръжените сили с личен състав, способен ефективно и ефикасно да изпълнява задачите по отбраната на страната и на съюзническите задължения в НАТО и в Европейските сили за сигурност.

Функциониращият модел за комплектуване на Въоръжените сили с военнослужещи в мирно време е валидизиран от Закона за отбраната и въоръжените сили на Република България /ЗОВСРБ/ и Правилника за прилагане на Закона за отбраната и въоръжените сили на Република България.

Правата и задълженията на военнослужещите произтичат от Конституцията и законите на страната.[1] Законовите разпоредби определят военната

служба като държавна служба с особено предназначение за подготовка и осъществяване на въоръжена защита на страната. Военната служба в мирно време се изпълнява като професия в Министерството на отбраната, в Българската армия и в структурите на пряко подчинение на министъра на отбраната, при условия и по ред, определени със ЗОВСРБ, ППЗОВСРБ, уставите на Въоръжените сили и със сключения договор за военна служба.

Осигуряването на въоръжените сили с човешки ресурси изисква привличането на кандидатите за приемане на военна служба да се извършва на основата на анализ и планиране на потребностите в съответствие с изграждането на необходимите оперативни способности.

Анализирането и прогнозирането се осъществяват на всички нива в Министерството на отбраната и Дирекция „Управление на човешките ресурси в отбраната“, като орган на стратегическо ниво, изготвя обобщен анализ за цялата структура, като съпоставя очакваните равнища на търсене и предлагане на работници и служители за организацията и определя техния количествен и качествен състав за съответния период.

Процесът на комплектуване с военнослужещи включва:

приемане на военна служба;

назначаване на длъжност и присвояване на военно звание;

преназначаване на по-висока длъжност;

преназначаване на равна длъжност;

преназначаване на по-ниска длъжност;

При комплектуването на въоръжените сили с военнослужещи се прилагат следните *принципи* в кариерното им развитие[2]:

откритост, прозрачност и информираност;

баланс между потребностите на въоръжените сили и личните интереси на военнослужещите;

съответствие на кариерното развитие на военнослужещите със структурата на въоръжените сили за постигане на необходимите оперативни способности;

обективност при оценяване на личностните качества и потенциала за развитие;

равнопоставеност по пол, расов, етнически и религиозен признак;

осигуряване на възможност за кариерно развитие на всеки военнослужещ;

Гражданите, приети на военна служба, са военнослужещи. Военнослужещите са офицери, офицерски кандидати, сержанти (старшини) и войници (матроси). Курсантите са военнослужещи с особен статус. При приемането на военна служба на военнослужещите се присвояват военни звания.

Механизмите за набиране на военнослужещи са различни за различните категории. Кариерата на военнослужещите се осъществява чрез назначаване / заемане на длъжности, изискващи равни или по-високи военни звания.

Длъжностите, по които се осъществява кариерното развитие на военнослужещите са:

във военни формирования/структури от състава на Въоръжените сили на Република България;

в състава на контингенти или отделни длъжности в мисии и операции извън територията на страната;

в международни организации и представителства извън територията на страната;

в международни организации и представителства на територията на страната.

Кариерното развитие на военнослужещите се изпълнява при смесен принцип:

чрез заемане на длъжности, които са обявяват в регистри на вакантните длъжности (либерален способ за преназначаване или преназначаване и повишаване във военно звание, при който военнослужещите кандидатстват за публично обявени длъжности и се определят от комисии за кари-

ерно развитие);
чрез заемане на длъжности, които се предлагат по прогнозно-планов способ (консервативен способ за преназначаване или преназначаване и повишаване във военно звание, при който военнослужещите се назначават на длъжности по предложение на командирите/ началниците /ръководителите).
Общите изисквания за приемане на пълнолетни български граждани на военна служба са залегнали в ЗОВСРБ[3] и те са :
да имат висше образование по специалността, за която кандидатстват - за офицерите, и средно или по-високо образование - за офицерските кандидати, сержантите (старшините) и войниците (матросите);
да не са по-възрастни от 40 години - за офицерите, 33 години - за офицерските кандидати и сержантите (старшините), и 28 години - за войниците (матросите);
да са годни за военна служба;
да не са осъждани за умишлено престъпление от общ характер, независимо от реабилитацията;
срещу тях няма образувано наказателно производство за умишлено престъпление от общ характер;
да нямат друго гражданство;
да не са освобождавани от военна служба поради наложено дисциплинарно наказание „уволнение";
да покриват нормативите за физическа годност, определени с акт на министъра на отбраната;
да са психологично пригодни.
Годността за военна служба се определя от военномедицински органи при условия и по ред, определени с акт на министъра на отбраната. Психологичната пригодност за военна служба се определя от специализирани звена и органи по психологичното осигуряване при условия и по ред, определени с акт на министъра на отбраната. Министърът на отбраната може да определи длъжности за войници (матроси), които да се заемат от лица с основно образование, когато за заемане на длъжността не се изисква достъп до класифицирана информация. Министърът на отбраната може да определи длъжности за военнослужещи, които да се заемат от български граждани с двойно гражданство, при спазване на изискванията на Закона за защита на класифицираната информация.
На военна служба могат да се приемат и лица, изпълнявали военна служба (кадрова военна служба), отговарящи на изискванията на общите изисквания с изключение на изискването за възраст ако: не са били освободени по дисциплинарен ред; към датата на приемане на военна служба им остават не по-малко от 5 години до навършване на пределната възраст за военното звание, изискващо се за заемане на длъжността;[4] кандидатстват за заемане на длъжността не по-късно

от 10 години след освобождаването от военна служба (кадрова военна служба).

Лицата, които притежават военно звание по резерва, съответстващо на званието на длъжността по длъжностното разписание, се приемат на военна служба с притежаваното военно звание, а на тези, които притежават военно звание по резерва, по-високо от изискващото се за длъжността, се присвоява военното звание, изискващо се за длъжността по длъжностно разписание. Същите подписват декларация за съгласие. На лицата, които притежават военно звание по резерва, с една степен по-ниско от изискващото се за длъжността, и са изпълнили изискванията за повишаване във военно звание, докато са били на военна служба, се присвоява военното звание, изискващо се за длъжността по длъжностно разписание.[5]

Механизми за набиране на офицери във въоръжените сили

Набирането на офицери за нуждите на въоръжените сили се осъществява следния порядък:

от завършилите висши военни училища в страната и чужбина, граждански лица;

от завършилите висши военни учебни заведения в страната военнослужещи (офицерски кандидати, сержанти и войници).

от завършилите висши училища граждански лица или военнослужещи – за длъжности, за които висшите военни училища не подготвят кадри;

приемане на служба на офицери, изпълнявали военна служба.

Основния механизъм за набирането на офицерите за нуждите на Българската армия се реализира във военните училища и Военната академия. За времето на обучение те придобиват необходимата военна, специална, лидерска и академична подготовка. Академичната подготовка съответства за придобиване на образователно-квалификационна степен „бакалавър" в професионално направление „военно дело" и образователно-квалификационна „бакалавър" или „магистър" от друго професионално направление за военните училища и образователно-квалификационна степен „магистър" по военно дело за Военна академия. На успешно завършилите висши военни училища в страната и чужбина, се присъжда диплома за висше образование за образователно-квалификационна степен „бакалавър", присвоява им се първо офицерско звание „лейтенант" и се назначават на длъжност командир на взвод или приравнена такава във военните формирования от въоръжените сили. Завършилите Военна академия военнослужещи по правило се назначават на длъжности изискващи старши офицерски звания (майор, подполковник или полковник).

За обучение в български висши

военни училища се приемат[6]:
за курсанти – редовна форма на обучение – граждански лица, притежаващи средно образование – за придобиване на висше образование на образователно-квалификационна степен „бакалавър" по специализации от специалност „Организация и управление на военни формирования на тактическо ниво" от регулираната професия „Офицер за тактическо ниво на управление";
за военнослужещи – задочна форма на обучение - офицери, притежаващи професионална квалификация по военно дело, офицерски кандидати, сержанти/старшини и войници/матроси - по специализации от специалност „Организация и управление на военни формирования на тактическо ниво" от регулираната професия „Офицер за тактическо ниво на управление";
За обучение във Военна академия „Г. С. Раковски" се приемат офицери, отговарящи на изискванията на наредба № Н-5/25.01.2018 г.[7] Обучението е в следните направления и форми на обучение: по специалността „Стратегическо ръководство на отбраната и въоръжените сили",в редовна форма на обучение; по специализации от специалността „Организация и управление на военни формирования на оперативно ниво", в редовна форма на обучение; по специализации от специалността „Организация и управление на военни формирования на оперативно ниво", в задочна форма на обучение. Завършилите офицери придобиват образователно-квалификационна степен „магистър" по военно дело и същите могат да заемат длъжности съответно, за които се изискват висши и старши офицерски звания. За военнослужещи офицери със специалности, за които не се провежда обучение във военните училища (например юристи, лекари, геодезисти, метролози, метеоролози, психолози, диригенти и др.), се приемат граждани, придобили висше образование с образователно квалификационна степен „бакалавър" и по-висока със съответна квалификация. Законът позволява с такива граждански лица да се сключат договори за обучение и същите по време на обучението си да бъдат стипендианти на министерството на отбраната. Непритежаващите военна подготовка, провеждат обучение във висшите военни училища, за придобиване на военна квалификация[8]. На приетите на военна служба се присвоява офицерско звание „лейтенант" и се назначават на длъжност от министъра на отбраната.
Допълнителни механизми за набиране на офицери с цел преодоляване на некомплекта във въоръжените сили са:
обучението във висшите военни училища на офицерски кандидати, сержанти/старшини и войници/матроси с висше образование за придобиване на професионална квалификация по военно дело.[9]

Военнослужещите, придобили тази професионална квалификация, могат да заемат длъжности за „капитан“ („капитан-лейтенант“), определени в Класификатора на длъжностите на военнослужещите в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия по чл. 24 от Закона за отбраната и въоръжените сили на Република България, до придобиване на образователно-квалификационна степен „бакалавър“ в професионално направление „Военно дело“[10];

обучение на военнослужещи във Военна академия, отговарящи на изискванията на § 99 и § 100 от преходните и заключителни разпоредби към Постановление № 191 на Министерски съвет от 2017 г. за изменение и допълнение на Правилника за прилагане на Закона за отбраната и въоръжените сили на Република България. Тази възможност съществува до учебната 2021/2022 г. Завършилите офицери придобиват образователно-квалификационна степен „магистър“ по военно дело и същите могат да заемат длъжности, за които се изискват старши офицерски звания;

приемане на военна служба и назначаване на длъжност на военнослужещи – офицери, изпълнявали военна служба в съответствие с изискванията чл.141, ал. 6 от ЗОВС. По този механизъм могат да се назначават офицери, както с младши, така и със старши офицерски звания. Назначаването на такива длъжности е на базата на организиране на конкурс.

Процедурата за организиране на конкурс е еднаква за всички категории военнослужещи и тъй като този начин на попълване е основен за войнишкия/матроски състав, то тя подробно ще бъде разгледана по-надолу в изложението, при разглеждане на механизмите за набиране на войници/матроси.

Преназначаването на военнослужещите на друга длъжност също би могло да се разглежда като един от механизмите за набиране на военнослужещи. Този механизъм макар и не директно оказва влияние при комплектуването на длъжностите – за останалата вакантна длъжност се търси попълнение. От друга страна преназначаването на длъжности способства за кариерното развитие на военнослужещите, което се явява един от мотивиращите фактори за служба във Въоръжените сили.

Кариерното развитие на офицерите се осъществява чрез заемане на длъжности в кариерни области и полета. Кариерните области и полета са: командни и професионални.

Кариерна област „командна“ обхваща длъжностите, изискващи младши офицерски звания и военно звание „майор“ („капитан III ранг“), определени в акт на министъра на отбраната, и придобита военна специалност и спе-

циализация във висшите военни училища.

Кариерна област „професионална“ обхваща длъжностите, изискващи младши офицерски звания и придобита гражданска специалност от висши граждански училища.

Кариерно поле „командно“ обхваща длъжностите, изискващи старши офицерски звания, с изключение на длъжностите, изискващи военно звание „майор“ („капитан III ранг“), определени в акта на министъра на отбраната по ал. 3, и придобита образователно-квалификационна степен „магистър“ в професионално направление „Военно дело“ от Военна академия или приравнена на нея в чужбина.[11]

Кариерно поле „професионално“ обхваща длъжностите, изискващи старши офицерски звания и придобита образователно-квалификационна степен „магистър“ по гражданска специалност от висши граждански училища. Гражданските специалности за кариерна област „професионална“ и за кариерно поле „професионално“ се определят с акт на министъра на отбраната.

Проблеми и перспективи за набирането на военнослужещи

за нуждите на Въоръжените сили

През последните двадесет години въоръжените сили на Република България се намират в процес на реформа, която по своите мащаби, обхват и сроковe не е позната в нашата история. Динамиката на провеждане на реформата, драстичното съкращаване в кратки срокове на числения щатен състав, привеждането на структурите в съответствие с новите изискванията и запазването на добре подготвените специалисти от всички категории военнослужещи, доведе до възникване на проблеми, свързани с организационното изграждане и развитие на въоръжените сили и Българската армия, а така също и с големия процент некомплектуваност на военната организация.

Реформата беше предвидена за реализиране в четири етапа, за времето от 1996 до 2020 г.:

Първи етап /1996 - 1998 г./ - разработи се 15 (петнадесет) годишна програма и през 1998 г. се прие „План 2010” с който стартира реформата.

Втори етап /1999 - 2004 г./ - през 1999 г. се прие „План за организационно изграждане на Българската армия до 2004 година” (План 2004), актуализиран през 2001 г.

Трети етап /2005 - 2015 г./ - през 2004 г. се прие „План за организационно изграждане и модернизация на въоръжените сили до 2015 година” (План 2015), актуализиран в последствие неколкократно.

Четвърти етап /2016 - 2020 г./ - през 2015 г. се прие „План за развитие на въоръжените сили до 2020 г.” (План 2020).

Извършените анализи на организационното изграждане и развитие на Въоръжените сили, както и на практиките и резултатите от тяхното изпълнение през тези етапи, показаха наличието на следните предизвикателства, при въздействието им върху военната мощ:

от поставените цели е реализирана само тази за съкращаване числеността на армията, без да са постигнати намеренията тя да бъде по-модерна, по-мобилна и по-боеспособна, оперативно съвместима с армиите от НАТО. Забавено е изпълнението на Целите на въоръжените сили/Целите на способностите, договорени с Алианса;

Таблица № 1. Времеви етапи на реформата във Въоръжените сили на Република България

№ по ред	*Етап на реформа*	*Времеви хоризонт*	*План за развитие*
1.	Първи етап	1996 - 1998 г.	План 2010
2.	Втори етап	1999 - 2004 г.	План 2004
3.	Трети етап	2005 - 2015 г.	План 2015
4.	Четвърти етап	2016 - 2020 г.	План 2020

приетите параметри на силите и програмите за тяхната модернизация надхвърлят значително икономическите възможности на страната;

разходването на бюджета за отбрана е извършвано без необходимата прозрачност и плановост, което е доведе до значително изоставане в технологичното модернизиране и оперативната съвместимост на Българската армия. Това изоставане натрупва непоносими за бюджета суми за поддържане на необходимите и още повече, за създаване на нови способности;

мащабът и динамиката на реформата изискват усъвършенстване на нормативната уредба, регламентираща организационното изграждане и развитие на въоръжените сили.

Възникналите проблеми се проявиха в следните направления: дублиране на функции между Министерството на отбраната и Генералния щаб (понастоящем Щаб на отбраната) на Българската армия, а впоследствие и в интегрираното министерство; не напълно уточнени функции и задачи на структурите от оперативното ниво на управление; определяне на организационните структури на базата на предварително спуснати квоти от личен състав; определяне на длъжности с цел запазване на добре подготвените специалисти от всички категории военнослужещи; създаване на органи-

зационни структури за кадрово развитие.

Причините довели до проблемите са както от обективен, така и от субективен характер. По-съществените от тях са: честа промяна в нормативната уредба; драстично намаляване в кратки срокове на числения щатен състав; липсва нормативен акт за систематизиране на правилата за извършване на организационното изграждане на военните формирования; промени в параметрите на длъжностите за военнослужещите без актуализиране на нормативните актове, в съответствие с измененията.

В началото на второто десетилетие на XXI век, благодарение на „мъдрото" политическо ръководство на въоръжените сили, умело прикрито зад всички по-горе цитирани планове и постановления и щедро подпомагани от все по-силно търсещи политическа изява военни, Българската армия е изправена пред най-голямото изпитание в своята история[12].

Съществуващата „секретност" допълнително ограничава прозрачността в сферата на политиката за сигурност и на разходите за отбрана. Така икономическите дейности на министерството достигнаха невиждани мащаби, доминиращи над отбранителната политика. Прозрачността стигна до пълно затъмнение.[13]

От 01.01.2008 година с окончателното отпадането на наборната военна служба и преминаването изцяло към професионална армия се промени и начина на попълване на личния състав в армията. Излизайки на пазара на труда всяка една организация в това число и Въоръжените сили трябва да се съобразяват с икономическия механизъм при търсенето и предлагането на работната сила т.е. какво е заплащането на труда. Военнослужещите имат право на основно месечно възнаграждение в съответствие с присвоеното им военно звание и длъжност в обхвата на военното звание.

Размерите на основното месечно възнаграждение се определят с акт на Министъра на отбраната. Базата за определяне размера на основното месечно възнаграждение за най-ниската длъжност се определя ежегодно със Закона за държавния бюджет на Република България, като това възнаграждение се увеличава с коефициент спрямо базата, както следва:

за офицери - не по-малко от 2,3%;

за офицерски кандидати и сержанти - не по-малко от 1,75%;

за войници (матроси) - не по-малко от 1,6%.

Базата за изчисляване на заплатите на военнослужещите е 380 лв. и тя е доста под размера на минималната работна заплата за страната, която в за 2018 година беше 510 лв.[14] Същата сума е залегнала и за 2019 година[15], като размера на минималната работна заплата в страната за 2019 годи-

на вече е 560 лв. Всичко това създава предпоставки за неатрактивност и неконкурентоспособност на военната професия на пазара на труда.

В Доклад за състоянието на отбраната и Въоръжените сили за 2016 г.[16] е направен следния анализ на окомплектоването на Въоръжените сили и причините за това. В него е посочено, че „Процентите на окомплектоване и тенденцията за увеличаване на некомплекта, особено в Българската армия, който за две години от 10% е достигнал до 20%, будят растяща тревога. Проблемът е особено силно изразен в по-малките и специализирани за конкретна дейност формирования, където броят специалисти е ограничен по длъжностно разписание и липсата дори на един от тях се отразява чувствително на боеспособността. Проблемни за попълване са и длъжностите, които не са свързани с даване на дежурства. Очертаващият се дефицит от кадри води до срив в подготовката и загуба на приемственост между поколенията, особено във високотехнологичните военни специалности. Заедно с ресурсните ограничения и остарялата техника, дефицитът на кадри поставя формированията пред сериозни предизвикателства при тяхната подготовка, поддържането на бойна готовност и способности за изпълнение на по-сложни в технологично и тактическо отношение бойни задачи.

Основните причини за проблемите с попълването на Въоръжените сили с личен състав са:

ниското заплащане, особено за войнишките длъжности, което прави войнската професия неконкурентноспособна на пазара на труда;

честите промени в нормативната уредба на системата за отбрана, незадоволителното социално положение на военнослужещите, несигурността относно тяхното бъдеще, дължаща се на липсата на ясни и точни правила и критерии за кадрово развитие;

не се осигуряват финансови средства за обявяване на конкурси за свободните длъжности;

демографски проблеми, поради който в гарнизоните, в които се обявяват конкурси, не се явяват достатъчно кандидати, а голяма част от явилите се, не успяват да покрият изискванията за здравен и психологически статус, или се провалят на теста за интелигентност.

От анализирането е видно, че една от причините за некомплекта е ниското заплащане. Стъпка в правилната посока би било промяна в начина на изчисляване на основната заплата на военнослужещите, като базата за определянето на възнаграждението да бъде обвързана с минималната работна заплата за страната.

В хода на разработването на тази статия се проведоха мероприятия за промяна на начина на заплащане на труда

на военнослужещите. Беше променен Закона за отбраната и въоръжените сили в частта му, касаеща заплащането на военнослужещите и се приеме нов „Класификатора на длъжностите на военнослужещите в Министерството на отбраната, структурите на пряко подчинение на министъра на отбраната и Българската армия“, в който да залегне „новата, стара философията“ – заплащането да е сбор от притежавано военно звание и заемана длъжност, като по този начин се цели възнаграждението да е според йерархичното нивото на заеманата длъжност, отговорностите, произтичащи от нея и притежаваното военно звание (до 2003 г. заплащането-заплатата на военнослужещите също беше на основата сбор на заплата за военно звание и заплата за заемана длъжност). Това само по себе си е справедливо разпределение на заплащането според спецификата на службата и отговорностите, но вътре в системата. За привличането на външни за системата лица, заплащането, което се предлага трябва да е съизмеримо със заплащането, което предлагат другите организации.

Следващата причина за некомплекта във Въоръжените сили е, че финансовите средства се планират на база списъчен състав на военните формированията/структурите, а не на брой военнослужещи по длъжностни разписания. Ниският процент на окомплектованост продължава да бъде сериозно предизвикателство за някои от формированията на Въоръжените сили. Попълването с личен състав е затруднено тъй като все още финансовите средства се планират на база списъчен състав на формированията/структурите, а не на брой военнослужещи по длъжностни разписания. Поради липса на достатъчен финансов ресурс, към настоящия момент, не е възможно да бъдат обявени конкурси за всички вакантни длъжности.

Това съществено влияе на способностите на Въоръжените сили защото в разработените длъжности разписания на военните формирования изискващите се способности се обезпечават със съответния брой длъжности по длъжностно разписание. От друга страна течащият през последните години процес на съкращаване на личен състав доведе много военни формирования до невъзможност да изпълняват своите функции. В желанието да се достигнат заложените параметри за личен състав, извършваните съкращения не бяха съобразени с очакваните способности на военните формирования.

Продължаващото преструктуриране на Въоръжените сили и съкращаване на личен състав пречи и на адекватното планиране на човешките ресурси във времето, особено за планиране на необходимия брой офицери. Набиране на кандидати за висшите военни

училища се основава на предварителни заявки от съответните потребители на кадри по специалности и специализации. В следствие на непрекъснатите съкращения заявките от потребителите на кадри бяха сведени до минимум, като в годините имаше специализации, за които не бяха правени заявки. В резултат на това по някои специализации не се подготвят кадри и са загубени способности от военно-образователната система за тяхната подготовка, тъй като преподавателите по тези специалности са пенсионирани или са се специализирали в преподаване на по-атрактивни специалности.

При заявяването на бройки за офицери е необходимо да се отчитат два основни момента, а именно:

времето за подготовка – периода на обучението е със срок 4 години т.е. приетите курсанти във военно-образователната система могат да се „ползват“ от потребителите на кадри след 4 години;

направената заявка сама по себе си не решава проблема с всички вакантните длъжности, защото:

няма гаранция, че за обявените места за обучение ще има кандидати;

вакантните длъжности в армията не са само и единствено за завършилите военни училища т.е. за лейтенанти, а са и за длъжности изискващи следващи военни звания. За да бъдат попълнени тези длъжности военнослужещите трябва да престоят определени години в съответното военно звание и освен това да преминат допълнително обучение и квалификация.

От организационна и финансова гледна точка е изключително трудно да се провежда обучение на отделни единици обучаеми по различни специалности. Имайки предвид съществуващите реалности на дневен ред все по-остро се поставя въпроса за адаптирането на този метод към новите условия на средата, с цел подобряване процеса по набирането на кандидати.

Един възможен подход е да се запази сегашното положение за специалностите, по които се обучават повече курсанти, а специалностите за които потребностите са изключително малки (1, 2 или 5 човека) да се закрият. Обучението на тези специалисти би могло да се извърши в други страни, макар че този подход би бил насочен с цел финансова целесъобразност, но ще доведе до загуба на национална способност в дадена предметна област.

Недостатъкът на този вариант е в няколко посоки:

В организационен аспект, така се лишаваме от възможността да развиваме военната наука във всичките й области, създавайки реална опасност да се загуби ценен преподаватели и научен потенциал в дадената област на военната наука.

Във финансов аспект, това ще стру-

ва повече от обучението в страната, предвид разликите в стандарта на живот у нас и във водещите във военното образование страни.

Не на последно място трябва да се отчита факта, че обучението в друга страна е свързано с *подготовката за използване на дадените кадри в чужда среда* и при други схващания за използване на Въоръжените сили, които не отчитат в пълна степен националните особености.

Един от важните въпроси на набирането на военнослужещи е изграждане на ефективна и гъвкава система за привличане на кандидати за военнослужещи във Въоръжените сили. Проблемите, които е необходимо да бъдат разрешени от органите по управление на човешките ресурси в това направление произтичат най-вече от динамично променящата се структура на изграждане на Въоръжените сили. В условията на наборната армия не е било необходимо да се използват каквито и да са методи за привличане на качествени кандидати за Въоръжените сили. По силата на закона всички граждани е следвало да бъдат на разположение на органите по личен състав. От тях се е изисквало да ги приемат и назначат на длъжности съгласно предварителната им подготовка и образование.

В новите условия на професионална армия, органите по управление на човешките ресурси се налага да се конкурират с другите организации за привличане на качествените и добре образовани кадри. В съществуващите условия на такава конкурентна надпревара се изисква да бъдат разработени нови методи за привличане на необходимите кадри за Въоръжените сили.

На *първо място* е необходима стройна система, която да определя отговорностите на органите на различни нива по привличането на кадри, както и начините за взаимодействие. Тя следва не само да регламентира дейностите по принцип, но и да бъде своевременно адаптирана за всяка отделна кампания за привличане на кандидати.

На *второ място* е необходимо да се отбележи важността на използването на всички средства за масова информация за издигане ролята на Въоръжените сили, като фактор в живота на държавата, популяризиране на службата във Въоръжените сили и перспективите от обучението във Висшите военни училища. Тази стъпка е изключително важна имайки предвид, че другите бизнес организации и университети също имат много активна позиция в търсенето на качествени кандидати за свои организации.

На *трето място* много важно за успеха на дейността по набиране на кадри е работата с училищата и бюрата по труда. Целта на тази дейност е от една страна, младите хора да научат за същността на Въоръжените сили и

условията за служба от самите представители на Министерството на отбраната или Българската армия. Така се избягва неточно или недоброжелателно показване на действителността на военната служба и обучението във Висшите военни училища. Провежданата подготовка за усвояване на знания, свързани със задълженията по отбраната на страната, действията за оцеляване при кризи от военен характер, както и за мисиите и задачите на Въоръжените сили, на учениците от 9 и 10 клас в изпълнение на изискванията за Закона за резерва на Въоръжените сили на Република България е стъпка в тази насока. От друга страна, работата с бюрата по труда дава възможност за реализация и на социалната функция на Въоръжените сили.

В заключение трябва да се посочи важността на администрирането на целия процес по набиране на кадри. Процедурата по подаване на документи, тяхната обработка и провеждане на подбор трябва да бъде бърза и лесноразбираема за кандидатите. Особено важно е да се избегне финансовото натоварване на кандидатите за служба във Въоръжените сили. В много случаи кандидатите за служба във Въоръжените сили или за обучение във Висшите военни училища не са сред най-заможната част от населението и необходимостта за подаване на документи или явяване на интервю на голямо отдалечение може да се окаже съществена пречка. Например пътуването до отдалечен град и разходите за престой в него е възможно да се окажат съществена пречка за набирането на кандидат с добра мотивация, здравословно състояние и образование. Това налага използването на пълните възможности на регионалните структури, които се ръководят от органите по управление на човешките ресурси, както и възможностите на информационните технологии.

Организационното изграждане на въоръжените сили е труден и скъпо струващ път, който трябва да извървим. Път, минаващ през дефиниране на понятия, като национални ценности, приоритети и интереси, с определяне на мястото на Въоръжените сили в тях.[17]

Политиката по управление на човешките ресурси е философията на въоръжените сили за човешките ресурси – какво е отношението, какъв е стилът на управление, какви са принципите и как се реализира тази философия. Като цяло политиката по управлението на човешките ресурси са средствата за постигане на целите на организацията и е очевидно, че те трябва да бъдат широко прокламирани, за да се говори за прозрачност и обективност на кадровият процес.

(Endnotes)

1 Симеонов, Т. Правна уредба на мениджмънта на сигурността и отбра-

ната, Военна академия „Г. С. Раковски“, София, 2014, ISBN 978-954-9348-50-7-7433,с. 22.
2 Доктрина за управление на човешките ресурси, чл. 124.
3 Закон за отбраната и въоръжените сили на Република България чл.141.
4 Пак там, чл. 160.
5 Правилник за прилагане на закона за отбраната и въоръжените сили на Република България, чл. 15.
6 Наредба № N-11от 2 май 2018 г. За условията и реда за приемане на курсанти и военнослужещи във висшите военни училища.
7 Наредба № N-5 от 25 януари 2018 г. За условията и реда за приемане на слушатели във Военна академия „Г. С. Раковски“.
8 Димов, П. Христозов, И. Перспективи за прилагане на иновационните технологии във Военна академия „Г. С. Раковски, VII-та национална конференция по електронно обучение във висшите училища, ISBN 978-954-07-4509-1, Софийски университет
9 Наредба за изменение на Наредба № N-19 от 25 май 2010 g. За условията и реда за приемане за разработването и планирането на курсове за придобиване, повишаване на квалификацията и преквалификацията, както и за кандидатстването на военнослужещи и цивилни служители от МО, структурите на пряко подчинение на министъра на отбраната и Българската армия за обучение в тях, Глава 4“а“.
10 Правилник за прилагане на закона за отбрана и въоръжените сили на Република България, чл. 16 ал. 2..
11 Пак там, чл. 115, ал. 2.
12 Лазаров, В. Военна сигурност – предизвикателства и перспективи, сп. Международни отношения год. XXXIX 2010 г. бр. 1-2, с. 68.
13 Рачев. В. Интегритет в отбраната: ефективни, прозрачно и отговорно управление, София, 2009 г.
14 www.kik-info.com/spravochnik/mrz.php.
15 http://www.minfin.bg/bg/1234.
16 Доклад за състоянието на отбраната и Въоръжените сили за 2016 г..
17 Лазаров, В. Ретроспекция на отбранителните способности на водещите сили на НАТО, сп. Международни отношения, година XL 2011 г., бр. 1. с.

Колективна защита срещу кибератаки – проблеми и възможности

Автори: Тотко Симеонов, Владимир Кабаиванов

Полковник доц. д-р Тотко Симеонов СИМЕОНОВ

Резюме: *Подходът при изграждането на новите методи и форми за колективната защита срещу кибератаки е в пряка зависимост от приоритизирането на новите заплахи за сигурността, породени от възможностите за използване на новите технологии за въздействие върху обществото. Колективната, както и националната киберсигурност трябва да гарантира защитеността на информацията, компютърните мрежи и свързаните с тях технологии.*

Ключови думи: *киберпространство, киберсигурност, киберзащита, кибератаки, колективна защита.*

COLLECTIVE PROTECTION AGAINST KIBERATAS - PROBLEMS AND OPPORTUNITIES

Abstract: *The approach to develop new methods and forms of collective defense against cyber-attacks is directly dependent on the prioritization of the new security threats posed by the use of new technologies to influence society. Collective, as well as national cyber-security, must ensure the security of information, computer networks and related technologies.*

Key words: *cyberspace, cybersecurity, cyber-defense, cyber-attacks, collective defense*

Информационните и комуникационните технологии са навлезли трай-

но в промишлеността, финансовия и банковия сектор, държавната администрация, военната област и др., тъй като улесняват изпълнението на ежедневните дейности. Този факт в съчетание с глобализацията, повишаващите се изисквания за по-бърз пренос на все по-големи по обем данни между потребители, както и по-широкото използване на Интернет наложиха компютърните системи като основно, стратегическо средство за комуникация, което функционира в специфична виртуална среда – т. нар. киберпространство. Отделният индивид, фирма, държава или международна организация зависят все повече от тази среда, което предполага нейното постоянно разширяване. По данни на Световния икономически форум от 2012 г., около 35% от населението по света е свързано с Интернет с 5 млрд. електронни уктройства. Тенденциите сочат, че през следващите 5 години потребителите ще се увеличат с 10%, а устройствата ще достигнат до 15 млрд.

Зависимостта между киберпространството и съвременното общество оказва влияние върху ролята и възможностите на виртуалния свят да въздейства във физическия[1]. Това пространство се разглежда като среда за обработване, съхраняване и обмен на информация, създадена от комуни-

кационни и информационни системи на физически или юридически лица, които осъществяват публични функции, и от връзките между тях и потребителите. Същевременно уникалните особености на киберпространството (виртуална среда, анонимност, бързина на действие, достъпност и т.н.), липсата на национални и законодателни граници в съчетание с възможностите на съвременните технологии улесняват нелигитимния достъп до информация предназначена за ограничен кръг от потребители. Това позволява извършването на нерегламентирани дейности или т. нар. киберзаплахи – прихващане и кражба на данни, подправянето им, целенасочени атаки за блокиране на елементи от критична инфратруктура, извличане на класифицирана информация и др. Появявя се нова среда в която се преплитат и противопоставят геополитически, икономически, социални, етнически, религиозни и военни интереси. Всичко това налага прилагане на комплексен подход, надхвърлящ възможностите на отделна държава и организация, при който да се изградят ефективни национални и международни способности за противодействие, както и прилагането на мерки за колективна защита.

Терминът „**киберпространство**“ (cyberspace) за първи път е ползван от американски писател, който описва с него област на колективни компютърни комуникации. Често това понятие се асоциира и с термините „виртуална реалност“, „дигитално пространство“ и др.

Съгласно учебник на Командването по подготовка и доктрини на САЩ киберпространството е *абстрактна или въображаема среда в която цифровизирана информация циркулира между мрежи от компютри*.

Може да се каже, че то обхваща цялата област от информационни ресурси, налична чрез компютърни мрежи. Включва всички елементи на компютърни системи, мрежи и технологии, както и бази с данни. Сложната, разнообразна и постоянно разширяваща се среда на кибепространството способства за появата на предизвикателства и заплахи към циркулиращата в него информация. Поради тази причина няма тяхна точна класификция. Правени са опити от отделни експерти или компании, занимаващи се с компютърна защита.

Според експерти спецификата на киберпространството и новите заплахи водят да поява на нова фронтова линия, както и нови димeнсии за военни действия, които са разположени извън традиционното бойно поле. Противникът се стреми да придобие дистанционен контрол и да управлява високотехнологични системи или техни елементи, включително и с военно предназначение. Това принуди редица страни и международни орга-

низации да предприемат конкретни мерки за защита от кибератаки, като:
инициране на законодателни промени/адаптиране на регламентиращи документи;
избор на подходящ модел на мениджмънт на способностите за защита;
създаване на специализирани органи за предупреждение, противодействие и минимизиране на щетите от кибератаките;
разширяване на двустранното, регионалното и международното сътрудничество.

Колективната, както и националната киберсигурност трябва да гарантира защитеността на информацията, компютърните мрежи и възаните с тях технологии. В тези направления водещите държави и международната общност инвестират значителен финансов, технологичен и човешки ресурс.

В световен план няма унифицирана дефиниция за киберзащита или киберсигурност. Съгласно Стратегията за киберсигурност на ЕС: *„тя обикновено се отнася до самозащита и дейности, които могат да се прилагат за защита на кибернетични пространства, както във военната така и в гражданската области, от тези за-*

плахи, които се асоциират или могат да навредят на самостоятелна компютърна мрежа и информационна инфраструктура."

Може да се обобщи, че *същността на киберзащитата включва комплекс от активни и превантивни мерки за опазване на информацията от атаки, като се изисква познаване и разбиране на източниците на заплахи*. В по-широк аспект това са мероприятия, процеси и технологии, които обезпечават устойчивото функциониране на конкретна система, която взаимодейства с киберпространството и предотвратяват насочени към нея киберзаплахи[2]. Последните са труднопредвидими поради спецификата на киберпространството, но анализът им показва зависимостта им от следните външни и вътрешни фактори – таблица:

Според експерти по киберсигурност, включително от НАТО и ЕС, киберзаплахите са идентични както за международни организации, така и за отделна държави. Чрез кибератаки противникът се стреми да постигане на желан краен резултат, а именно достъп до характеристиките на цифровата информация и по-точно нейната конфиденциалност, достъпност, достоверност и автентичност.

Конфиденциалност – ползване на информацията по предназначение и амо от определен кръг потребители;

Достъпност – възможност за нейното ползване съобразно изискванията на потребителя;

Достоверност – предотвратяване на възможности за нейното манипулиране;

Автентичност – гарантиране за по-

Фактори	
Външни	***Вътрешни***
Интереси на държави, структури и субекти	Неблагоприятна социална и икономическа среда
Стремеж за доминиране в киберпространството	Ръст на претъпността
Дейност на терористични и екстремистки организации	Липса/не актуализирани регламентиращи документи
Разузнавателни служби	Ограничени финанси
Технологичен дисбаланс	Неефективни способности и механизми за управление на киберзащитата
	Ниско ниво на технологии и подготовка на персонала

следния, истински вариант на информацията.

Във военната област този вид защита трябва да съхранява собствените системи от т. нар. „информационни оръжия" на противника, които са предназначени за поразяване/унищожение на информационните системи в рамките на информационни операции и включват най-вече електронна война (EW) и операции в компютърни мрежи (CNO) и др.

Електронната война по своята същност цели да подтисне част от спектъра използван от противника и успоредно с това да предпази сегмент от него, който се ползва от собствената КИС. CNO включват два вида дейности, които са насочени към защита на компютърните мрежи (Computer Network Defence) и атаки на компютърни мрежи (Computer Network Attack). Първите касаят защитата на собствените компютърни мрежи, а вторите – разкриване и противодействие на противниковите КИС.

За справяне с предизвикателствата на международно ниво се разработват принципи и норми за намаляване на уязвимостта на компютърните мрежи и стриктно регламентиране на достъпа до информация. Създават се способности, които да бъдат в състояние да противодействат ефективно на кибератаките с възможности за засичане, предупреждение, превантивни действия, противодействие и бързо възстановяване. Въпреки това с развитието на технологиите се наблюдава и постоянно усъвършенстване на методите за търсене на незащитени места и технологични пропуски в национални и международни КИС, с акцент върху тези с военно предназначение[3].

Проблемите пред колективната киберзащита се свързват главно с киберзаплахите с акцент върху кибератаките и организирането на адекватна защита. Първоначално тези въпроси се разглеждат на експертно национално ниво. Добиват популярност през последните години след поредица от кибератаки, насочени към: *обекти от критичната инфраструктура* (бразилски ВЕЦ, 2005-2007 г. и системи за индустриален контрол в Иран, 2010 г.); *институции* (министерства в Естония и посолството на САЩ в Талин, 2007 г.); *специфични информационни масиви и бази с данни*, съдържащи класифицирана и некласифицирана информация (Пентагона, 2007 г.); *държавни и частни телекомуникационни и информационни мрежи* (Германия, 2007 г.), и др.

Заплахите са свързани със софтеурни или технически пропуски, които дават възможност за случаен или целенасочен нерегламентиран достъп до информация, която се създава, обработва, съхранява и пренася в електронна среда. В зависимост от своята природа и способи за атакуване, могат условно да се разделят на 3 вида:

1) причинени от природни бедствия и аварии;

2) произтичащи от конкретна среда, неизправности и отказ на технически средства, дефектирал хардуер.

3) причинени от човешка намеса (преднамерена и непреднамерена).

Непреднамерените са в резултат на намеса от служители на организацията, експлоатираща мрежата поради: *недоволство,* персонал извършва саботажни дейности, подтиквани от лични причини и неудовлетворени служебни амбиции; *случайни пробиви*, причинени несъзнателно от служители поради техническа некомпетентност.

Преднамерените са свързани с лица в или извън организацията, които предимно чрез хакерска атака опитват нерегистрирано проникване. Мотивите им могат да бъдат политически, икономически, социални, религиозни и др. с цел корпоративен или държавен шпионаж, лично облагодетелстване и т.н. При атаката се ползва специално разработен софтуер за скрито дистанционно подчиняване на конкретната информационна система, източване, модифициране на конфиденциални данни или изтриване на данни като обикновено се предизвиква:

- *Претоварване на компютърна система и нарушаване на нормалното й функциониране* чрез заразяване с вирус или троянски кон - отказ на услуга (Denial of Service);
- *Подчиняване на мрежа от софтуерни приложения или компютри* с цел кражба на лични данни - Ботнет;
- *Нанасяне на щети на даден компютър* чрез „злонамерен софтуер“ (малуер) - троянски коне, червей или вирус;
- *Кражба на лична информация* с Интернет измама (Фишинг) чрез електронно съобщение/фалшив сайт.

Според експерти, всеки ден в света циркулират около 150 000 компютърни вируса, които компрометират 148 000 компютъра. От финансова гл.т. се оценява, че през това десетилетие престъпленията в киберпространство ще причинят щети за около 200 млрд. евро.

Потенциален проблем за надеждността на компютърните мрежи може да бъдат човешкия фактор или самите потребители и поддържащия персонал. За намаляване на рисковете световната практика ограничаване на достъпа чрез принципите за „необходимост да се знае“ и „минимални права“.

Специфичен проблем е дейността на терористични и екстремистки ор-

ганизации в глобалната мрежа. Те са оценили предимствата на електронните медии и ги ползват за пропагандиране на идеи, информиране на привърженици, манипулиране на общественото мнение, набиране на финанси, привличане на поддръжници, планиране и координиране на действия, дезинформация, отправяне на заплахи и психологически операции.

Според специалистите обаче, за **първостепенен проблем** може да се счита комплексна кибератака, инициирана от държава, след предварителна подготовка, значителни финансови и технологични инвестиции, водеща се от няколко направления и съчетаваща различни способи върху една цел.

Според статистически данни, само през миналата година в НАТО са регистрирани 2500 опита за нерегламентиран достъп. Тези събития ускориха адаптирането на **регламентиращата база, модифицирането на механизма за мениджмънт и изграждането на способности за защита**. Процесите са съобразени с политико-военния характер на организацията и гарантирането на колективната отбрана на страните.

Алиансът разполага с концепция (МС 0571/2008 г.), дефиниции на понятия (киберотбрана, кибервойна, кибератака, киберпространство), механизъм за мениджмънт и др. Осъвременяването на регламентиращата база се активизирана през последните години в: *Стратегическата концепция* (ноември 2010 г., Лисабон), определяща кибератаките като заплаха за информационните и комуникационни системи и средата за сигурност; *Концепция за киберзащита за повишаване на киберсигурността* (2011 г.), която набляга върху развитие на собствени способности, разширяване на сътрудничество с партньори, международни организации и отчитане на киберзаплахите в процесите на планиране на отбраната; ***Политиката на НАТО за киберзащита*** (2011 г.), с визията, приоритетите, целите и общите задачи. Беше приет и План за действие за киберзащита с начините и конкретния инструментариум за осъществяването на политиката[4].

За практическо прилагане на регламентиращите документи НАТО разполага със следната структура:

Фигура 1. Управление на киберсигурността в Алианса (съгласно Политиката на НАТО за киберзащита).

Бордът на НАТО за управление на киберотбрана (the NATO Cyber Defence Management Board) е основният координиращ орган, който разпределя дейностите между цивилните и военните структури и взема решения на стратегическо ниво. Включва експерти в политическата, военната, техническата и други сфери, които имат отговорности в направление киберотбрана. За изясняване на технически въпроси и аспекти от прилагане на документацията се ползва експертиза от Борда за консултации, командване и контрол (NC3 Board). Изпълнението на оперативните изисквания, придобиването и внедряването на техническа екипировка е поверено на Агенцията на комуникации и информация (NCIA).

Възможностите за колективна защита на Алианса се изразяват в :

Практически способности – изградени са няколко групи за бързо реагиране. Всяка с ядро от шестима души и готовност за действие до 24 часа от началото на инцидента. Те оказват помощ при поискване от всяка страна членка, след одобрение от Северноатлантическия съвет (САС) и страните членки. Могат да подпомагат страните както с практическа защита, така и с обучение на специализирани национални звена;

Ползване на аналитичния потенциал за предупреждение и оценка на киберзаплахи. Задачи в това направление изпълняват: *управление „Операции и разузнаване“* в SHAPE (оперативно ниво); *аналитични структури в Цен-*

търа на НАТО за обединяване на разузнавателна информация (Молесуърт, Великобритания) оперативно и стратегическо ниво; за нуждите на САС и Военния комитет се ползва *Съвместната дирекция „Разузнаване и сигурност"* в която са обединени експерти от Международния и Международния военен секретариати;

Механизъм за предупреждение чрез възможностите на Системата на НАТО за отговор на кризи (NATO Crisis Response System). Тук са съвместени способностите на Системата на НАТО за разузнавателно предупреждение (NATO Intelligence Warning System), информация по линия на цивилните национални специализирани органи и ситуационен център в SHAPE;

Провеждане на специализирани учения в които се отработват въпроси, свързани с дейностите при компютърни атаки както на работно („Кибер коалиция") така и на най-високо ниво, при което се разглежда и управлението на кризи (Crisis Management Exercise – CMX). При последното учение бяха разгледани въпроси и отработени действия свързани с превантивни мерки и преодоляване на последици от атаки на елементи от критичната инфраструктура на отделни страни членки и опит за физическо проникване в компютърните мрежи на Главната квартира;

- възможностите на Центъра за изследване, изграждане и развитие на способности за сътрудничество в областта на киберзащита (NATO Cooperative Cyber Defence Center of

Excellence). Основните му задачи обхващат разработването на стандарти в областта на киберзащита на Алианса, изготвянето на експертизи в случаи на кибератаки и обучение и тренировка на специалисти от съюзни и партньорски държави.

Европейският съюз също е цел на кибератаки. Съюзът отчита влиянието на Интернет и киберпространството върху всички аспекти на обществото и произтичащата необходимост от киберзащита. Дейностите в това направление са в синхрон с принципа за наложен пацифизъм. Усилията са насочени към изготвяне на регламентиращи документи, изграждане на способности, насърчаване на сътрудничеството между страните и разширяване на отношенията с други организации. Акцентът е колективна защита основана на термина „устойчивост“ (resilience) на комуникациите. За защитата и гарантирането на фундаментални права, демокрацията, прилагането на законите и т.н. в киберпространството Европейската комисия публикува *Стратегия за киберсигурност* и директива за мрежовата и информационната сигурност (МИС), а Стратегията „Отворено, безопасно и сигурно киберпространство” (2012 г.) съдържа визия на ЕС за постигане на колективна киберзащита чрез: устойчивост на информационните системи; прилагане на мерки за намаляване на киберпрестъпността; водене на активна международната политика в това направление; дефиниране на основни понятия като киберсигорност[5] и киберпрестъпност[6]. Дейностите за постигане на високо ниво на сигурност ще се извършват при съблюдаването на 5 принципа:

Основните ценности на ЕС важат както за физическия така и за виртуалния свят;

Защита на основните права, свободата на изразяване и личната информация;

Достъп на всеки гражданин на Евросъюза до Интернет;

Демократично и ефективно многонационално управление.

Споделяне на отговорностите за гарантиране на сигурност.

Те ще се реализират при съсредоточаване на усилията за изпълнение на 5 приоритета:

Постигане на устойчивост в киберпространство - с активно сътрудничество между ЕС, правителствата на страните членки и частния сектор и ползване на собствени способности. ЕС изгради през 2004 г. Европейска агенция за мрежова и информационна сигурност (ENISA), която отговаря за защитата на критичната информационна инфраструктура, събира данни, анализира на рисковете, повишавава информираността и популяризира опита за управление на риска. Освен това се предвижда работа за:

определяне на минимални изисквания към МИС на национално ниво.

Предвижда се създаване на механизми за управление с функциониращи стратетегии и действащи Екипи за отговор при инциденти в областта на информационната сигурност (CERT). Такъв екип е сформиран като постоянна структура през 2012 г.;
изграждане на механизми за превенция, засичане и отговор на киберзаплахи;
повишаване на нивото на готовност и степен на участие на частния сектор. За целта през 2009 г. беше създадена платформа „Европейско партньорство на обществени и частни структури за устойчивост“ за обмен информация и опит;
повишаване на познанията - чрез ежегодното специализирано учение „Кибер Европа“ (Cyber Europe) с участие на частния сектор.

Намаляване на киберпрестъпността. Според дефиницията тя се отнася за широк спектър от криминални дейности, в които са включени компютри и информационни системи като основна цел или инструмент. ЕС счита, че е една от най-бързо развиващите се форми на общата престъпност, чието ограничаване може да се постигне с:
повишаване на ефективността на законодателството. Страните се насърчават да приемат Конвенцията на Съвета на Европа за киберпрестъпността (т. нар. конвенция от Будапеща). Предстои приемането и на директива на ЕС за атаки срещу информационни системи;
усилване на оперативните способности за борба с киберпрестъпността[7] Страните могат да ползват финансови инструменти за 2013 г. по програмата „Превенция и борба с престъпността“, а след това от фонда за вънрешна сигурност (Internal Security Fund). Предлага се и възможност за обмен на практически опит и експертизи от Европейския център за борба с киберпрестъпността (ЕС3) в рамките на Европол.

Разработване на политика за киберзащита и способности, свързани с общата политика за сигурност и отбрана (ОПСО). Европейските експерти предлагат изграждането на способности за киберзащита да бъдат фокусирани върху засичането, отговора и възстановяването от съвременни киберзаплахи. Положително въздействие би оказало обединяването на гражданския и военния подход в това направление. За да избегне дублирането на усилия и неефективното изразходване на материални ресурси, ЕС е предприел действия в посока подобряване на оперативните способности на съюза, използвайки добрите практики и опита на НАТО в тази посока, с акцент критичната инфраструктура;

Разработване на промишлени и технологични ресурси за киберсигурност. ЕС отчита зависимост от информационни компоненти произведени в трети страни. За преодоляването й се

предвижда:
промотиране на общ пазар на продукти за киберсигурност;
насърчаване на инвестициите за изследвания, развойна дейност и иновации. За целта е разработена Рамкова програма за изследвания и иновации „Хоризонт 2020“, която ще стартира през 2014 г. под надзора на ЕК. Програмата ще подкрепя изследвания в областта на новите информационни технологии, предлага решения за тяхната сигурност, подпомага постигането на оперативна съвместимост и др.;
Водене на съгласувана международна политика за киберпространството и насърчаване на основните ценности на Евросъюза. Предвижда се използването на потенциала на страните членки, ЕК и Върховния представител по въпросите на външните работи и политиката на сигурнос, както и разширяване на струдничеството с ООН, Съвета на Европа, НАТО, ОССЕ и др.
Евросъюзът планира разширяване на сътрудничеството между ENISA, Европол и Европейската агенция за отбрана. В случай на престъпление оперативното ръководство ще се поема от Евпорол/ЕС3 с помощ от правозащитните органи на засегнатата държава/-и. При констатиране на кибершпионаж или държавно подкрепяна компютърна атака, ще се информират националните специализирани и военни органи за организиране на своевременна защита. Препоръчва се страните членки да разполагат с необходимите стратегии, структури за кибернетична защита и борба, както и да се насърчава частния сектор с цел по-добро разбиране на природата на тези заплахи.
Еволюцията на технологиите ще продължава, което ще увеличи и зависимостта на индивида и обществата от сложни информационни системи. Процесът е съпроводен от съответни предизвикателства, които също ще се развиват и модернизират. Киберзаплахите са труднопредвидими и имат наднационален характерТе стават по-чести, по-мащабни и по-сложни без да се съобразяват с границите във физическия свят. Могат да причинят значителни щети в национален, регионален и глобелан план, като заплахата стои в дългосрочен план.
Сложният и променлив характер на киберпространството улеснява провеждането на кибератаки от една страна, като от друга затруднява и оскъпява изграждането на ефективна киберзащита. Ползването на колективни механизми съчетава националните способности за противодействие с тези на съответната организация. Променливата природа на заплахите налага координирани усилия и превантивни мерки за гарантиране на сигурността на колективното информационно пространство, както и бързо адаптиране на регламентиращи документи, гъвкави механизми за

управление и адекватни способности за киберзащита.

(Endnotes)

1 Димов, П. Приложение на уеб технологии за защита на националната сигурност, ISBN 978-954-2977-47-6, Диомира, 2018

2 Стойков, С. Маринов, Р, Лазаров, Л. Кочев, Я. „Изграждане на системата за ранно реагиране на система за ранно регистриране на кибер защити“, Сборник доклади от годишна конференция на НВУ „В. Левски“ 2014, том 2 с.159-168, ISSN 1314-1937.

3 Лазаров, В. Новите реалности и разузнаване с хора, Изток-Запад, 2012, ISBN 619152051-4, с. 169.

4 Стойков, С. Маринов, Р, Лазаров, Л. Кочев, Я. „Информационните войни и политиката на НАТО за кибер защита“ Сборник доклади от годишна конференция на НВУ „В. Левски“ 2014, том 2 с. 145-157, ISSN 1314-1937.

5 Иванов Г. Концептуални аспекти на киберсигурността, Сборник научни трудове, ISBN 978-954-9681, Шумен, 2014, с. 269.

6 Лазаров, В. Матрични решения за националната сигурност, Изток-Запад, 2012, ISBN 619152096-4, с. 216.

7 Ivanov G., Cybersecurity of mobile devices, KSI Journal Knowledge Society, Number 1, Veliko Tarnovo, ISBN 2367-7198, 2015, p. 24 – 27.

Симеонов Т., „Аспекти на усъвършенстването на подготовката на офицерите за осигуряване с информация на многонационални щабове в операции различни от война” – Конференция на факултет „Командно -щабен“, Военна академия „Г. С. Раковски“ 2006, ISSN 1312-2991

Кибернетична сигурност и кибернетична война, Center for Strategic and International Studies - Vashinkton, 2011, [cited 08.04.2013 г.], Available from: www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

Всеобхватния подход на ЕС към киберпространството, Velikobritania, Germania, Shvecia I Holandia, 2012 г.

Стратегия за киберсигурност на ЕС, [cited 06.04.2013 г.], Available from: https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52013JC0001

Симеонов Т. Правна уредба на мениджмънта на сигурността и отбраната, Военна академия „Г. С. Раковски“ 2014, ISBN 978-954-9348-50-7

Защита срещу кибер атаки [cited 06.04.2013 г.], Available from: http://www.nato.int/cps/en/SID-980C535B-FF50380D/natolive/75747.htm

Усъвършенстване на способностите в областта на Кибер защитата [cited 06.04.2013 г.], Available from: https://www.ccdcoe.org/

Информацията и националната мощ

Автор: Подполковник д-р Живко Желев

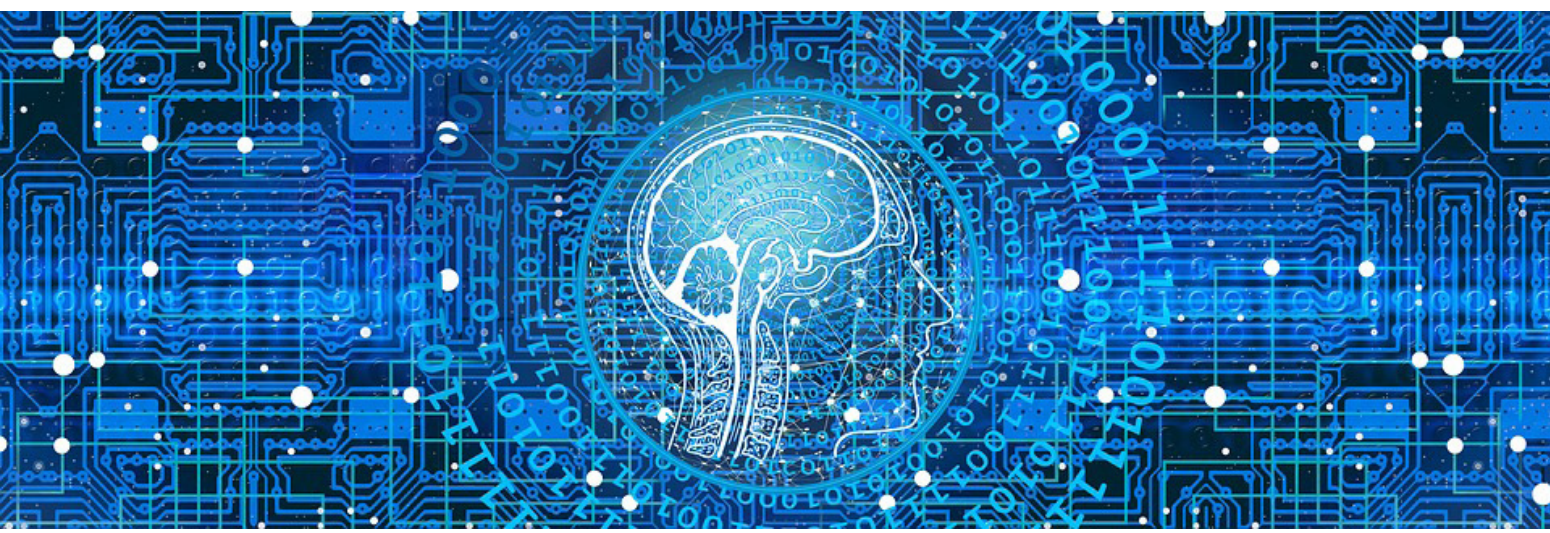
Zhivko Zhelev. INFORMATION AND NATIONAL POWER

Статията представя зараждането и развитието на информационното въздействие като елемент на бойна мощ Въз основа на което е направен анализ на предпоставките за възприемането на информацията като елемент на националната мощ.

The article presents the emergence and development of the information impact as a component of combat power. Based on which an analysis was made of the prerequisites for the perception of information as an element of national power.

***Key words**: Information, Information Operation, National Power*

В съвременната високотехнологична епоха, информационния елемент на силата се възприема от мнозина, като решение на множество проблеми. Поради което политическите ръководства на страните са разбрали значението на информацията, като елемент на националната и военната мощ, а военно ръководство е възприело редица информационни дейности, като средство за генериране на допълнително национална и военна мощ[1]. Развиването на способности за информационни операции в рамките на военната структура и непрекъс-



нато усъвършенстване на тактиките, техниките и процедурите за информационни операции, се възприема като елемент на упражняването на властта, а загуба в борбата за информационно превъзходство може да има непредсказуеми последици.

В доктрината за информационни операции информационното превъзходство се определя, като оперативно преимущество, извлечено от способността да се събира, обработва и разпространява непрекъснат поток от информация, като не се позволява или ограничават способностите на противника да извършва аналогични дейности[2]. Разбира се, това превъзходство не е постоянно и не е гарантирано.

С появата на държавите, информационното противоборство се превръща в съставен елемент на техните взаимоотношения, не само във военно време, но и в мирно време, както и в борбата за вътрешно политическа власт и влияние. Развитието на информационното противоборство е свързано с появата на нови и все по-достъпни средства за разпространение на информация, под чието въздействие се вземат решения. По този критерии, можем да говорим за четири основни етапа на информационното противоборство: вербален;

книжен; технически; телекомуникационен. При това всеки следващ етап възприема и доразвива средствата и методите на предходния.

Военачалниците от древността са установили че е възможно да се противопоставят на противниците си не само с военни средства, но и с психологически, които значително снижават бойният потенциал на противника. Поради което воюващите са се опитвали да използват средства за духовно въздействие, за да отслабят морала и бойната мощ на противника и да повдигнат бойният дух на собствените войски.

В ***първият етап*** на информационно въздействие, човекът е основен носител на информацията и обект на въздействие, посредством психиката му, определяща неговото поведение. Не случайно Аристотел още в 4 век пр. н. е. е определил онези области от човешката психика, които се явяват обект на информационно въздействие – съзнание, воля и чувства. Способите за водене на информационно въздействие са били ограничени до използване на вербални техники, поради високата неграмотност на населението. Подобни техники са включвали ораторски речи, религиозни проповеди, слухове, дезинформация, демонстрация на военно превъзходство, всяващи страх стенописи (знаци), арести, публични физически наказания (екзекуции) и др. Важен обект на информационно въздействие се явяват духовните служители, като най-образовани и ползващи се с влияние върху народните маси.

Вторият етап на информационното въздействие настъпва с масовото разпространение на грамотността, в условията на широко разпространение на печатни издания и използването на хартията като средство за съхранение и разпространение на информация. През този период се появява и едно ново и използвано до наши дни средство за въздействие - листовката. Други съществени изменения в този етап са появата на новите транспортни средства - параходите и влаковете, значително повишаващи скоростта на придвижване. Разширява се наборът от средства за физическо повлияване в условията на информационно въздействие, включващи взривове и палежи на издателства, типография, закриване на редакции, изгаряне на книги, списания, листовки и др.

Третият етап на информационното противоборство започва с появата на нови носители на информация, обусловени от откриването на електричеството (втората половина на 19 в.) и включва използването на фотографии, телеграфи, радио и пр. Значително се увеличава нагледността и формирането на образи при информационното въздействие. Увеличават се възможностите за натрупване и продължително съхраняване на ин-

формация в значителен обем. Създават се възможности както за избирателно така и за масово влияние върху чувствата емоциите и съзнанието на хората. Всичко това стой в основата на информационната война, осигуряваща постигането на външнополитически, стратегически цели посредством управлявано информационно въздействие върху индивидуалното и групово съзнание на противника.

През този етап се създават информационно-техническите средства за въздействие върху информационната инфраструктура и информационните потоци на противника – средствата за електронна война. Тези средства позволяват да се лиши противника от възможности за своевременно предаване и получаване на информация, необходима за вземане на решение. Така се заражда и развива информационно-техническото направление за информационно въздействие широко използван в периода на първата и втората световна война.

Четвъртият етап започва с появата на персоналните компютри (средата на 70-те години на 20 в.) и междудържавните телекомуникационни мрежи. Това позволява да се провежда скрито информационно въздействие, както персонално върху конкретен човек, така и неконтролирано върху широката общественост. Следователно широко се увеличават възможностите за провеждане на координирано информационно въздействие. Появата

на програмно-техническите средства позволява да се използват и програмни продукти, нарушаващи нормалната робота на компютри, компютърни мрежи и др. програмни устройства и системи. Появяват се компютърните вируси, като широко приложимо информационно оръжие[3].

За този етап са задължителни следните условия: наличие в противостоящите страни на определено ниво на компютъризация на информационната инфраструктура, компютърна грамотност и свободен достъп до глобалната компютърна и телекомуникационна мрежа, наличието на програмно-технически средства за защита и нападение на двете страни.

Въпреки че различните елементи на информационните операции са били прилагани в цялата история на военното дело, по време на Първата световна война се прави систематизиран опит за организиране на усилията в областта на информацията. Контрола на трансатлантически комуникации е предоставил на съюзниците предимството в контрола на информационния поток за въздействие, спрямо „Централните сили". Създадената в този период от правителството на САЩ ***Комисията по обществена информация***, се превръща в инструмент за управление на пропагандната като количество и място за прилагане, за да се повлияе на световната и национална аудитория[4]. Използвайки стратегическите комуникации, комисията по обществена информация е осъзнала критичната роля на информацията

и възможните задачи, за които може да се използва в интерес на военните усилия на страната.

С напредъка на Първата световна война необходимостта от по-големи способности на летателните апарати е била очевидна. Комисията по производство на въздухоплавателни средства на САЩ разработва програма имаща за цел да се повлияе на политически елит на страната, за да се осигури одобрението и оказването на необходимата подкрепа на зараждащата се авиационна индустрия. За нуждите на тази програма са пряко ангажирани усилията на различни американски медии. Крайният резултат е един президентски подпис, осигурил необходимите средства и подкрепа.

По време на Втората световна война правителството на САЩ, създава служба „***Военна информация***", имаща предназначение да оказва помощ при целенасоченото използване на информацията. Тази усилия в областта на използването на информация са били от жизненоважно значение за военните усилия на САЩ, отнасящи се до повлияването върху морала на американския народ и за укрепване на взаимоотношенията със съюзниците. Въпреки че пропагандните усилия на САЩ са били насочени към силите на Оста, разработването на програми за подпомагане на военните усилия е ясно насочена към американския на-

род. Основните информационни дейности в този военен период са били насочени към програмите за придобиване на военни облигации и доставянето на продоволствия, представянето на смелия американски войник и подлия враг от филмовата индустрия, а кратките новинарски клипове за американските победи са имали за цел да информират и да влияят на американското население. Тези усилия не са били информационни операции, но са форми на стратегическата комуникация, представящи използването на информацията през Втората световна война, от правителството на САЩ за собствените си цели[5]. Други програми са били насочени за неутрализиране на опитите на „Оста“ да повлияе на неутралните целеви аудитории и собствената от въздействието на пропагандната им машина. Въпреки постигнатите резултати същите са били прекратени поради обществените протести, настъпилото объркване относно стратегическите комуникации, информационни операции и усилията за информиране.

Нормативните документи от този период са позволявали или поне не са ограничавали командирите да използват информационни операции, за да се унищожи, разруши, ограничи, заблуди, използва, влияние, защити, открие, възстанови и отговори на противниковите опити за действие. Дефинирането на информационната терминология в общите условия допринася за объркването. Например, *пропаганда* е „всяка форма на комуникация в подкрепа на националните цели, предназначени да повлияят на становища, емоции, нагласи или поведението на всяка група, за да се възползва възложителя, но нито пряко, нито косвено”[6], *информационно осигуряване* е „интегрирано прилагане на обществени дейности, за информиране на собствените и приятелските аудитории, психологически операции, военни репортажи, стратегически комуникации в подкрепа и защита на публичната дипломация, както и други средства необходими, за да повлияят на чуждите аудитории, лидери и военнослужещи в подкрепа на общите усилия”[7], а *стратегическите комуникации* са „фокусирани правителствени усилия за ангажиране на ключови аудитории за създаване, укрепване или запазване на благоприятни условия за развитие на правителствените интереси, политики и цели, чрез използване на координирани програми, планове, теми, съобщения и продукти, синхронизирани с действията на всички инструменти на националната мощ”[8] или „координирани по подходящ начин дейности на НАТО в областта на публична дипломация, връзки с обществеността, военни връзки с обществеността, информационни операции и психологически операции и други, в подкрепа на политиката, опе-

рациите и дейностите на Алианса”[9]. Самото сравнение на тези определения показва неопределени граници, а дори и самият акт на информираност може да се разглежда като способност на информационните операции. Следователно своевременното информиране може да се превърне в мощно оръжие.

Значението на информация се разбира много добре от лидерите на противостоящите страни в комплексния характер на съвременното бойно пространство. Съвременните информационни технологии осигуряват незабавна и актуална информация, но това налага необходимостта от детайлен анализ, оценка и защита[10]. Отделят се огромни ресурси за защита на собствените компютърни мрежи, за информиране и повлияване на целеви аудитории, за синхронизиране на различни информационни усилия при постигане на желания краен резултат и за съзнателно нарушаване цикъла на вземане на решения на противника. Всички тези отделени ресурси имат за цел да подпомогнат информационните усилия за повлияване или ограничаване на достъпа до информация, необходима за ефективното вземане на решения от противостоящата страна. Но въпреки всичките усилия и отделени средства, информационните дейности остават все така разединени и не постигат желаните ефекти и резултати.

Развитието на ***стратегическите ко-***

муникации, информационното осигуряване, както и използването на обществените медии от противниците е довело до голямо разнообразие от гледни точки за това, как да бъде най-точно определен информационния елемент на мощта и как се вписва ролята на военните информационни операции в цялостните информационни усилия, за използване по най-добрият начин на информационните възможности на въоръжените сили.

За военните, създаването на собствени доктрини за информационни операции и обучение в тази област е бавен и съпроводено с редица трудности. Всеки вид въоръжена сила развива собствени способности за информационни операции, за да се гарантира, че въоръжените сили ще са достатъчно ефективни не само в традиционните военни конфликти, но и в операциите в отговор на кризи и в стабилизиращите операции. Този преход от традиционната война към борба с асиметрични заплахи (война) увеличава нуждата от военните способности в областта на информационните операции и необходимостта да се гарантира, че военните усилия са синхронизирани с цивилни информационни агенции. Въпреки че военните се фокусират върху развитието на способностите за информационни операции, то тези предизвикателства са тясно свързани с развитието на стратегическите комуникации[11].

Ефективното ***използване на информационните операции*** се основава на тяхното разбиране за същността им, техните елементи (инструменти и техники) и тясното взаимодействие помежду им за постигане на максимален ефект. Основните възможности на информационните операции се постигат посредством електронна война, операции в компютърните мрежи, психологически операции, операции по военна заблуда и операции по сигурността, без да се пропускат и възможностите на останалите елементи, които са свързани или подпомагат въздействието в информационната среда[12]. Това са дейности, които се отнасят предимно до вземащите решение или процеса на вземане на решение, като в същото време се защитават собствените аналогични процеси. Това е процес на интегриране и координиране на всички възможности на информационните операции, за да се постигне синхронизирано и фокусирано въздействие, като същевременно максимално се използват и ефектите или успехите на останалите инструменти и техники на информационните операции.

Информационните операции включват дейности за повлияване, нарушаване или узурпиране на състезателното вземане на решения, независимо дали е от хора или от автоматизирани системи, като същевременно се защитават собствените аналогични про-

цеси. Този процес не замества същността на конвенционалната военна мощ, а по скоро я подкрепя или засилва ефектите чрез синхронизиране на усилията. Определянето на информационните операции и ефективното им прилагане са два различни въпроса. Интегрирането на инструментите на информационните операции със стратегическата комуникация и публичната дипломация включва множество проблемни въпроси отнасящи се до правни предизвикателства, използването на комуникационни и компютърни технологии и възприемането им от обществото[13].

Актът на информираност е начин да се повлияе на конкретна целева аудитория, но информиране не означава, че целевата аудитория ще приеме информацията, независимо от нейната истинност. Неразбирането на информационните операции и процеса на повлияване са само някои от предизвикателствата пред състава пряко ангажиран с планирането и провеждането им. Способността да се балансира и координира информационния поток, подкрепен от конкретни действия е от ключово значение. Различните целеви аудитории изискват различни подходи за въздействие. Използването на възможности за определяне, информиране и повлияване в съгласувани усилия изисква синхронизирани действия, с цел максимално интегриране на информационното въздействие във всички правителствени и военни дейности за генериране на национална и бойна мощ.

Националната мощ е стратегическия ефект, който може да създаде държавата за единица време, в конкретна среда за постигане на желаното крайно състояние. Инструментите на националната мощ са средствата с които разполага държавата за постигане на националните цели, а те биват политически, военен, икономически, граждански и информационен.

Бойната мощ е елемент на военната мощ и е средство с разрушителната сила, която военните формирования могат да прилагат срещу противника в даден момент. Елементи на бойна мощ са маньовър, огнева мощ, лидерство, защита на силите и информация. Чрез анализ на относителната бойна мощ, се определят силните и слабите страни на противостоящите сили и възможните осъществими операции.

Както беше посочено, информацията е елемент на националната мощ, следователно информационните операции са приноса на въоръжените сили в подкрепа на националните и коалиционни информационни усилия. Демокрацията предлага свобода на словото и независимост на медиите, което предполага както представяне така и дискредитиране на идеи, лъжи, предразсъдъци и др. Предизвикателствата налагат необходимостта от предоставяне на информация

пред аудитория, която се определя като дезинформация за подвеждане или заблуждаване на противниците. Информационните операции предвиждат военните и правителствени ръководители да използват информацията, като оръжейна система, но балансирането на военни способности със стратегическите комуникации може да е объркващо. Доктриналната терминология допринася за объркването относно добиването и използването на информацията за нуждите на въоръжените сили и провежданите от тях операции. Използването на информация от военните е фокусирано върху потенциалния противник, да се наруши дейността му, като се влияе на цели и на канали използвани от противостоящите сили. Защита на собствени сили от противникови информационни дейности включва и предотвратяването на отрицателното влияние върху неутрални аудитории, което неутрализира един от безценните инструменти в арсенала на врага.

Потенциалните противници не са обвързани със съблюдаването на правни и етични изисквания, които собствените сили са задължени да спазват. Предизвикателство е когато медиите и обществеността не могат да правят разлика между информация, погрешна информация или дори дезинформация. Информационните операции предоставят ключова спо-

собност, която военните могат да използват, за да се противопоставят на погрешната информация и дезинформация или да използват възможностите си да влияят, да нарушат или узурпират цикъла на вземане на решения на противника. Потенциалното колебанието на съюзническите агенции да представят собствените си действия на неутрални или приятелски целеви групи, може да ни постави в явно не изгодна позиция.

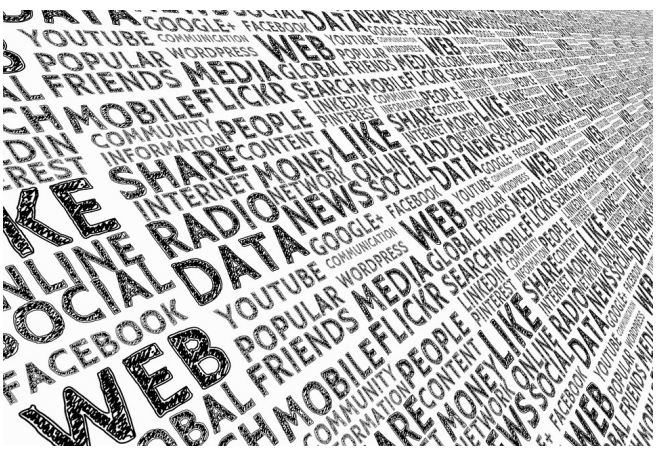
Съществен принос за успеха на информационните операции е способността им за предоставяне на консултации и координация на военните информационни дейности с цел да се създаде желания ефект върху волята, разбирането и способността на противници, потенциални противници и други участници в подкрепа на целите на операцията[14]. Наблюденията на различни военни и граждански организации, които са правили анализи на участието си в информационни

операции разкриват, че дейностите по информационните операции не се разбират от значителна част от гражданските и военните ръководители и е налице погрешно схващане, че информационните операции са само координирано прилагане на психологически операции, операции в мрежите и публична дипломация. Съгласно приетото определение, информационните операции са интегрираща функция на способности предоставяни от отделните инструменти и техники, прилагани за постигане на целите на операцията.

Въпреки че ***стратегическите комуникации не са специфична военна възможност***, влиянието им се усеща на всички нива на военните операции. Информацията служи като множител, който създава доверие в „думи, изображения и действия“, но информацията без подкрепата на действия е просто думи без стойност[15]. Стратегическите комуникации са едно от основните оръжия в борбата с невярната информация и дезинформацията на стратегическо ниво. Информационните операции са „военната ръка“ на националните и коалиционни информационни усилия, подкрепящи стратегическите комуникации и публичната дипломация чрез своите действия и съпътстващи информационни усилия. Ако стратегическите комуникации и военните послания са противоречиви, тогава доверието на обществеността е загубено.

Целта на стратегическите комуникации е да се осигури на обществото достоверна и навременна информация, която ще повлияе осигуряването на неговата подкрепа за постигане целите на управляващите и на военните операции. Много пъти военните са в ролята на комуникатори представяйки информация отнасяща се до военни действия, хуманитарни мисии или рутинни военни операции[16]. Военните организации трябва да знаят целите на стратегическите комуникации за подкрепа на националните и коалиционни усилия и да координират своите и гражданските дейности. Влиянието върху аудитории посредством съобщенията на стратегическите комуникации е от особен интерес за военните.

Следователно основната предпоставка за появата на информационните операции е възприемането на информацията, като елемент на бойната мощ и възможностите им за целенасоченото въздействие върху информацията



и информационните потоци, имащо за цел да се повлияе върху волята, разбирането за ситуацията и действията на целевата аудитория. Поради този причина информационните операции се превръщат от допълващи конвенционалните военни действия във водещи при реализирането на националните интереси в междудържавните отношения. Израз на всичко това е определянето на информацията като елемент на националната мощ.

(Endnotes)

1 FM 3-0, Headquarters Department of the Army, Operations, 2008, p. 69-75.

2 JP 3-13 Information Operations, 2012, p. 22-23.

3 Воронцова Л. В., Фролов Д. Б., История и современность информационного противоборства, Горячая линия Телеком, М, 2006, стр. 5-7.

4 Dennis Murphy and James White, Propaganda: Can a Word Decide a War?, Parameters 37, 2007, p. 17.

5 Edward Coffman, The War to End all Wars, Lexington: The University Press of Kentucky, 1998, p. 191-192.

6 JP 1-02, Dictionary of Military and Associated Terms, Department of Defense, April 2001, p. 441.

7 FM 3-0, Operations, Headquarters Department of the Army, February, 2008, p. 73.

8 JP 1-02, Dictionary of Military and Associated Terms, Department of Defense, November 2010, p.226.

9 AD 95-2, ACO Strategic communications, 2012, p. 4-10.

10 Димов, П. Приложение на уеб технологии за защита на националната сигурност, Диомира, 2018;

11 Irregular Warfare (IW), Directive 3000.07, U.S. Department of Defense, December 2008, p. 8.

12 JP 3-13, Information Operations, November 2012, p. 58-60.

13 Dr Dan Kuehl, Information Operations: The Hard Reality of Soft Power, Information Resources Management College, March 2014, p. 6-7.

14 AJP-3.10 Allied Joint Doctrine, for Information Operations, 2009, p. 23.

15 Dennis Murphy, Strategic Communication Wielding the Information Element of Power, U.S. Army War College, June 2008, p. 180.

16 James Stavridis, Strategic Communication and National Security, *JFQ*, 2007, p. 4.

Новите предизвикатества и подхода на функцията и способността гражданско-военно сътрудничество

Автор: Подполковник д-р Милен Кисьов

Анотация: Тази статия разглежда накратко новите изисквания и подход на тази функция и способност, наложени от промените в средата на сигурност и предизвикателствата на съвременния свят. Посочват се инициативите на центърът за ГВС на НАТО, вероятните нови области на приложението, както и развитието на обучението и подготовката на специалистите по ГВС.
Ключови думи: *гражданско-военно сътрудничество, предизвикателства,* взаимодействие, обучение, подготовка, *приоритети.*

THE NEW CHALLENGES AND THE APPROACH TO FUNCTION AND COMPETENCE CIVIL-MILITARY CO-OPERATION

Milen Kisyov, PhD

Annotation: This article briefly discusses the new requirements and approach of this function and ability imposed by changes in the security environment and the challenges of the modern world. It outlines the initiatives of the NATO CIMIC Center of Excellence, the likely new areas of application, as well as the development of the training and preparation of the CIMIC specialists.
Keywords: civil-military cooperation, interaction interactions, training, preparation, priorities.

Напрежението между Русия и балтийските страни, както и политико-военни съюзи и подобни образования, предизвикано от разполагането на ракети в Калининград, а също и влошаването на гражданската сигурност в редица страни поради важни и все още нерешени глобални и регионални проблеми, показва и довежда до невъзможност да се действа в такива нови условия, без да се коригират планове, готовности за действие и най-вече направления за обучение и подготовка на специалистите, работещи в различните сфери на противостоенията.
През октомври 2016 г., провежда сре-

ща с участници в трите балтийски държави, за да се обсъдят възможностите за ускоряване на гражданско-военната интеграция и взаимодействие в рамките на НАТО. В допълнение на това са разгледани влиянието над ГВС на растящата урбанизация и другите съвременни тенденции в сферата на сигурността. Не само гражданските общества трябва да коригират своите стратегии и процеси за планиране на непрекъснато променящия се свят. Военните специалисти имат също жизненоважна значение за да се посрещат солидарно предизвикателствата на времето. Срещите в Уелс и Варшава и решенията от тях преориентират фокуса на НАТО. Но какво означава това за съвместната военна функция на НАТО гражданско-военно сътрудничество (ГВС)?

Решенията от срещата на върха на НАТО във Варшава за промяна на план за готовност за действие (Readiness Action Plan-RAP) чрез увеличаване на военното присъствие на НАТО, подчертава стратегическото значение на балтийските държави.[1]

На фона на тези събития, през 2016 г. НАТО стартира Балтийската инициатива за ГВС.[2] Специалистите и експертите от центъра на НАТО за върхови постижения в областта на ГВС в Хага[3] не са встрани от тази инициатива и подчертават смисъла и значението на военната съвместна функция ГВС. В редица проведени работни срещи и бордове са обсъдени методите и подходите за по-нататъшно засилване и интегрирано прилагане на ГВС не само в Прибалтика, но и в НАТО като цяло. Този център действа като цялостен експертен хъб, обучаващ и разпространяващ знанието и осигурява място за срещи с ключовите партньори в колективната отбрана. Такива срещи между партньорите повишават и утвърждават новата способност гражданско-военно взаимодействие (ГВВ) във връзка с граждански, институционални и военните участници в трите партньорски прибалтийски републики.

В изявленията на директора на центъра Волфганг Паулик[4] се казва, че „ГВС е (реалната) подкрепа на сътрудничеството между суверенни държави. Във времена на криза и конфликти, според плана си за готовност за действие, НАТО е напълно готов да подкрепи балтийските държави-членки в запазването на териториалната им цялост и чрез улесняване на безопасна и сигурна среда. Това ще гарантира устойчивостта на законните граждански власти в суверенните общества на балтийските републики. Докато съюзът НАТО е много добър в постигането на военните цели във въоръжени конфликти, то той също прилага всеобхватно критериите за ефективно ГВС, за да се осигури сигурна и безопасна среда“.

Успоредно с това, продължава усъвър-

шенстването на тази съвместна функция чрез осигуряването на предметна експертиза по въпросите на ГВВ и ГВС, както и на сътрудничеството със структурите на силите на НАТО – звена като Първи немско-холандски корпус (Мюнстер), Многонационалният съвместен щаб (Улм) и Многонационалният корпус Североизток (Шчечин), които са неразделна част от плана за готовност за действие на НАТО за защита на балтийските държави. Обсъждат се перспективите и възможностите за по-нататъшно подобряване на балтийското гражданско-военното сътрудничество. Това се определя от разбирането, че само общи структури и общо разбиране на задачите осигуряват предварителните условия за ефективно сътрудничество по време на криза.

Ангажиментите на центъра за ГВС в Хага се насочват допълнително към устойчивостта на ГВВ при изпълнение на действия по колективната защита в условията на хибридна война. В тази връзка, именно тази балтийска инициатива на НАТО по отношение на ГВС, като първична за ГВВ функция, е реално и пряко насочена към засилване на взаимната помощ, осигуряване на експертиза и обучение от партньорите от НАТО. Директорът на центъра Паулик заявява, че „не може да има никакво съмнение, че вече сме в състояние на колективната отбрана на НАТО в рамките на един сценарий на хибриден конфликт, който се разиграва на фона на нашите граждански общества. Ето защо е ясна целта на нашите срещи с различни заинтересовани страни в трите балтийски държави, за да се запознаят всички наши партньори в колективната отбрана с необходимостта от участие на централните показатели на ГВС, техните дейности по планиране и учения, провеждани в зависимост от осигуряването, адаптацията и договорените мерки.[5] Експертите признават уникалния интерес към обучението и използването на функционалните специалисти по ГВС. Центърът обучава и тренира стотици такива експерти, като предоставя индивидуални програми за обучение.

Самият център за върхови постижения в областта на ГВС е мултинационална структура[6], акредитирана от НАТО и спонсорирана от основните участници в този център. По този начин се осигурява добавена стойност, иновации и навременни съвети, като и опит по почти всички въпроси на двете функции - ГВС и ГВВ - за граждански и военни „клиенти“. Основният фокус на центъра е засиленото обучение и подготовка на цивилни и военни служители в двете функции; концептуалното и доктриналното развитие на ГВС, както и поуки по ГВС от всички мисии на НАТО.

От друга страна, в съответните звена на НАТО за интеграция (NFIU) са обсъдени конкретни проекти за подобре-

ние на ГВС, насочени към повишаване на националните способности за осъществяване връзка между цивилното население, силите на НАТО и с гражданските международни организации.

В диалог с партньорите са обсъдени перспективите и възможности за по-нататъшно подобряване на ГВС в НАТО. Това се определя от разбирането, че само общи структури и общо разбиране на задачите осигуряват за предварителните условия за ефективно сътрудничество по време на криза. Като ангажимент на НАТО по отношение на ГВС, допълнително ще „засилват“ на място способността за устойчивост и противопоставяне на емитирането на елементи на въздействие на хибридната война, чрез повишаването способностите за гражданско-военно взаимодействие и за колективна защита. Оценките на другите, близки до ГВС функции се оказват все повече нужен за изучаване и прилагане инструментариум. Това се доказва от следната съпоставка:

„Това взаимодействие е полезен инструмент в подкрепа на дейностите и посланията на информационните операции. Действията му способстват „делата да се представят чрез думи“, които показват намерението на войсковите формирования, участващи в дадена операция. Взаимодействието между организациите[7], които са отговорни за гражданско военното сътрудничество и останалите играчи, като например различните международни, правителствени и неправителствени организации, са основен участник в процеса на обмен и координиране на информационните потоци. Информацията, придобита чрез рутинна операция по гражданско-военно сътрудничество е инструмент за идентифициране на ключовите целеви аудитории и на каналите за достигане до тях. Рутинните задължения на лицата, които участват в тези операции могат да играят значителна роля в цялостния процес на информационно осигуряване. Специалистите по гражданско-военно сътрудничество ежедневно взаимодействат с местното население и действията, произтичащи от това са значими. Липсата на синхрон с общите усилия в дадената информационна операция може да бъде катастрофално[8]. Въпреки, че не подкрепя пряко информационните операции, гражданско военното сътрудничество може да се възползва от усилията на информационните операции. Пред структурите, участващи в операции по гражданско-военно сътрудничество, са изяснени целите на цялостния процес и те оказват подкрепа на командирите. Често тези операции се провеждат самостоятелно или паралелно с информационните операции и публичната дипломация, но това е само едно от многото предиз-

викателства. Интеграцията на трите осигурява по-добри способности за обмен на съобщения. Способността на гражданско-военното сътрудничество да предоставя обратна информация на или за други информационни операции, по-специално на психологическите операции, също могат да повлияят на ефективността. Ползите от съвместно усилие осигуряват представянето на резултатите, постигнати от операциите по гражданско-военно сътрудничество."[9]

Нещо повече, като принос на този център към съвместната академична общност от институции за военни и цивилни специалисти, заинтересовани страни в областта на обучение за национална и колективна защита, центъра представи през 2017 г. своята академична магистърска специалност по гражданско-военно взаимодействие, което отговаря на все по-големия интерес по темата във военния и в цивилния сектор. Партньорите в колективната отбрана определят нуждата от редовно обучение и повишаване на квалификацията на допълнителен брой военнослужещи за нуждите на ГВС и ГВВ. Заедно с това, като резултати и изводи от срещите и реалностите, се препоръчва да се работи активно за кариерното развитие на екипите за ГВС, за търсенето на нови възможности за институционално взаимодействие и създаването на интерес в обществото. Това, според анализаторите, значително ще подобри способността за цялостното разбиране на обхвата на гражданско-военното взаимодействие в рамките на националните територии. Например, в Естония, експертите от центъра са особено впечатлени от дейността и ангажираността на естонските активни доброволни сили в подкрепата им за държавата в продължение на много години. В момента над 25 000 естонци подкрепят военните, полицейските и други основни държавни функции.

Изводът, който е нужно да се направи е, че първоначалните стъпки за изпълнение на Инициативата на НАТО за ГВС в Балтика през 2017 г. е представен най-добре от директора на центъра: „Ние съзнателно решихме да направим по-дълго пътуването през трите балтийски държави, с цел да се получат от първа ръка впечатление на хората, природата по отделните въпроси, както и интересите на всяка държава. Ние използвахме тази възможност, за да се ангажираме с длъжностни лица и различни местни хора, за да придобием възприятие на всеки от актуалните въпроси на сигурността, за които става въпрос днес." Всъщност, по този начин се прилагат характерните за специалиста по ГВС слогани – „Срещни се!, „Говори!", „Действай!".

Така, е удачно да се счита, че със своя принос центъра вече е напълно готов да отговори на задачите и целите, как-

то е посочено на срещата на върха на НАТО през 2016 г. В отговор на решенията, инициативата се насочва към подпомагане на съюзниците в североизточния регион.

Центърът за ГВС в Хага е натоварен със задачата да дава отговори на въпросите за бъдещата роля и значение на ГВС. За приложението на ГВС в рамките или в границите на териториите на страните може да се каже, че то ще бъде различно от прилагането му в далечно развръщане, в конфликтни региони и страни, дори и в провалени държави. Но винаги към тази способност и функция ще има изисквания за продължителна подготовка на персонала за мисии и операции и за да остане ГВС приложимо, трябва да бъдат дадени отговори на редица въпроси, да се дават съвети на тези, които ги търсят и всичко това - в стратегически посоки и рамки.

За се постигне такава добавена дейност, центъра преразглежда възможностите (неговите собствени, на партньорите и на участници от други страни) как да се изпълняват нарастващите задачи съобразно времето за действие и наличните ресурси. Поради това, се достига до извода за важността и нуждата да се разработят ново разбиране на ключовите приоритети на ГВС и ГВВ, както и за средствата и активите, необходими за правилното изпълнение с дълготраен ефект на тези и нови бъдещи задачи и предизвикателства.

Другият подход към ефикасността от дейностите по ГВС и действията на центъра е чрез задължителното осъзнаване и отговор на въпросите: „Дали правим правилните неща? И правим ли тези правилни неща по правилен начин?“ В помощ на този поход, се прави отсяване на наистина важните въпроси и проблеми. Концентрацията над тях и върху това, което е важно и което може да се направи сега, не трябва да оставя на заден план другите начини на действие и въздействие. Всъщност, тази стратегия се анализира в момента.

БЪДЕЩИ ПРИОРИТЕТИ В ОБУЧЕНИЕТО И ПОДГОТОВКАТА ПО ГВС И ГВВ

„Сътрудничеството между ЕС и НАТО за противодействие на хибридните заплахи е една от основните насоки за взаимно допълване на инструментите на мощта на двете международни организации и чрез които инструменти би следвало да се противодейства на заплахите на средата за сигурност. В първия доклад[10], свързан с напредъка по изпълнението на общия набор от предложения между НАТО и ЕС, десет от четиридесет и две предложения са свързани с борбата срещу хибридните заплахи. Двете международни организации, заедно с държавите-членки и съюзниците, с подписването на декларацията за изпълнението на общия набор от предложения имат амбицията да

допринесат и да участват в дейностите на Европейския център за противодействие на хибридните заплахи (ЕЦПХЗ), създаден в Хелзинки. Тук ключов момент се оказва по-добрата възможност за осведоменост за ситуацията, която се явява и от решаващо значение за навременното и ефективно противодействие на хибридните заплахи. Създаването на ЕЦПХЗ на ЕС и взаимодействието му с новосъздадения център за анализ на хибридните заплахи на НАТО ще помогне за изграждането на обща картина на ситуацията в Европа. Това ще способства за превантивни, адекватни и най-вече ефективни мерки срещу заплахите за средата за сигурност в Европа.[11]

Резултатите от непрекъснатото развитие на архитектурата на сигурност и разширяваща рамка на свързаните с тях теми, трябва да бъдат приложени и решени чрез обучение и подготовката на специалисти по ГВС. С цел те да бъдат в състояние да се установят приоритетите на съществуващите и нови теми, се провеждат редица проучвания и конференции, срещи и семинари в общността на интереси по ГВС и ГВВ. Резултатите от всички тези форуми и проучване довеждат до оформянето на нови приоритетни въпроси и действия[12], като най-известните от тях са:

1. Действия в условията на колективна отбрана.
2. Действия в условията на хибридни заплахи и противопоставяне.
3. Действия в подкрепа на гражданската готовност
4. Действия за защита на цивилното население.
5. Действия при управление на кризи.
6. Действия при неконтролируема емигрантска и хуманитарна криза.
7. Действия при извършване на ненасилствени дейности за смяна на властта.

Призванието на специалистите и експертите в тези две области е да работят активно в рамките на обучението и подготовката, за да се постигне състояние, в което ще е възможно вземането на адекватни решения за справяне с тези въпроси и проблеми. Затова своевременното адаптиране на обучение и образование по ГВС и ГВВ съобразно продължаващите динамики в архитектурата на сигурността е от първостепенно значение. Обучението на персонал, специалисти и експерти по тези две области ще е реално предизвикателство, но именно така ще се подобри ефективността от дейностите и задачите в различни и непривични досега домейни и области от средата на сигурност.

Сега, днес е времето, за да продължаване на развитието във всички държави-членки на структури и персонал, за да стане ГВС ключов показател и подкрепяща функция, които да са в непрекъсната ангажираност с всички

части на населението на страната, за усъвършенстване на уменията за ориентиране в такава ситуация, както и националната ангажираност и устойчивост.

Но с всичките тези нови предизвикателства – вътрешни и външни, някои области на съвместните граждан-ско-военните дейности ще бъдат натоварени с повече работа, а други - с по-малко. Ето защо е важно да се улесни създаването на баланс между тях, за да се гарантира, че центъра, специалистите и експертите, функционалните специалисти и анализаторите в обединената област на ГВС и ГВВ в съюзен формат, ще бъдат в състояние за в бъдеще да отговорят на всички предизвикателства, въпроси и проблеми.

(Endnotes)

1 NATO Policy for the Protection of Civilians, https://www.nato.int/cps/en/natohq/official_texts_133945.htm?selectedLocale=en

2 CIMIC MESSENGER, Civil-Military Cooperation Centre of Excellence, Volume 8 Issue 3, September 2016, https://issuu.com/ccoe_pao/docs/ccoe_cimic_messenger_2016-03

3 About us, Welcome to the CIMIC Centre of Excellence, https://www.cimic-coe.org/

4 The Baltic NATO CIMIC Initiative 2016, The CIMIC Centre of Excellence follows NATO Warsaw lead towards North-East.https://www.cimic-coe.org/about-cimic/the-baltic-nato-cimic-initiative-2016/

5 Baltic NATO CIMIC Initiative 2016 – Reviewed, https://www.cimic-coe.org/ABOUT-CIMIC/THE-BALTIC-NATO-CIMIC-INITIATIVE-2016/BALTIC-NATO-CIMIC-INITIATIVE-2016-REVIEWED/

6 Иванов, Г. Подбор, подготовка, оценка и развитие на служители във военна организация, Диомира, , ISBN 978-954-2977-49-0, 2018, София, с. 99.

7 Иванов, Г. Подготовка, отговорности, функции и задачи на военния аташе, Военен журнал, бр.1, 2014, ISSN 0861-7392, с. 130.

8 Димов, П. Приложение на уеб технологии за защита на националната сигурност, ISBN 978-954-2977-47-6, Диомира, 2018

9 Желев, Ж. Информационни операции и информационно въздействие, 2018, Монография „Военна академия“, ISBN 978-619-7478-01-03, с. 26

10 Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils from 6 December 2016,

https://eeas.europa.eu/sites/eeas/files/170614-joint-progress-report-eu-nato-en-1.pdf, p.

11 Георгиев, В. Източници на несигурност в Европа, влияещи върху средата за сигурност – причини, последствия и възможни решения.

12 Best Practice Template, https://www.cimic-coe.org/products/conceptual-design/downloads/ccoe-publications/ccoe-factsheets/

Специализиран брой: Римска история

Киберсигурност в дигиталния свят

Автор: Полковник доцент доктор Иван Чакъров

Анотация: *Работата анализира основните аспекти на киберсигурността в днешното широко използване на комуникационни и информационни технологии. По-долу са представени взаимовръзките между понятия като кибернетични атаки, кибер престъпления, които са в основата на дефиницията за киберсигурност. Посочени са общо приети функционални характеристики, критерии за качество на важността на кибератаките.*

Ключови думи: *киберпространството, кибератаките, интернет и информационните и комуникационни технологии, сигурната маршрутизация, критичната и информационната инфраструктура.*

CYBERSECURITY IN THE DIGITAL WORLD

Ivan CHAKAROV, PhD, Associate Professor, Colonel,
„Communication and Information Systems",
Department „Command and Staff" Faculty
Rakovski National Defense Academy,
Sofia, Bulgaria

Annotation: *The piece of work analyzes the main aspects of cyber security in today's extensive use of communication and information technologies. Below, the relationships between concepts such as cyber attacks, cyber crimes, which are the basis for the definition of cyber security, are given. Generally accepted criteria are indicated for functional features and quality of the importance of cyber attacks.*

Key words: *cyberspace, cyber attack, internet and information and communications technologies, critical and information infrastructure.*

Съвременният свят все повече въздейства на обществото в световен мащаб, като дигиталната обвързаност във

всички области създава условия за традиционно висок риск, но с различна интензивност през времето. С появата на интернет не всички потребители ползват виртуалното пространство за мирни цели. Ефективността на киберсигурността[1] е пряко свързана с нейното функциониране, и е фундамент за цялата кибер концепция и обществена практика. Това е безспорен факт, защото реализирането на нормативната база и практиките по осигуряване на комплексна система за защита може да предотвратят и отразят заплахите във виртуалното (кибер) пространството[2], чрез необходимата за това ресурсна („кибермощ“), субектна („киберспециалисти“) и институционална (държавни специализирани органи и политики и законова и нормативна база) обезпеченост[3].

Нейното постигане е свързано с всебхватно преосмисляне на проблемите на киберсигурността, формиране на адекватни на съвременните реалности концепции и осъществяване на система от взаимосвързани практически действия, водещи към изграждане на качествена система за защита.[4]

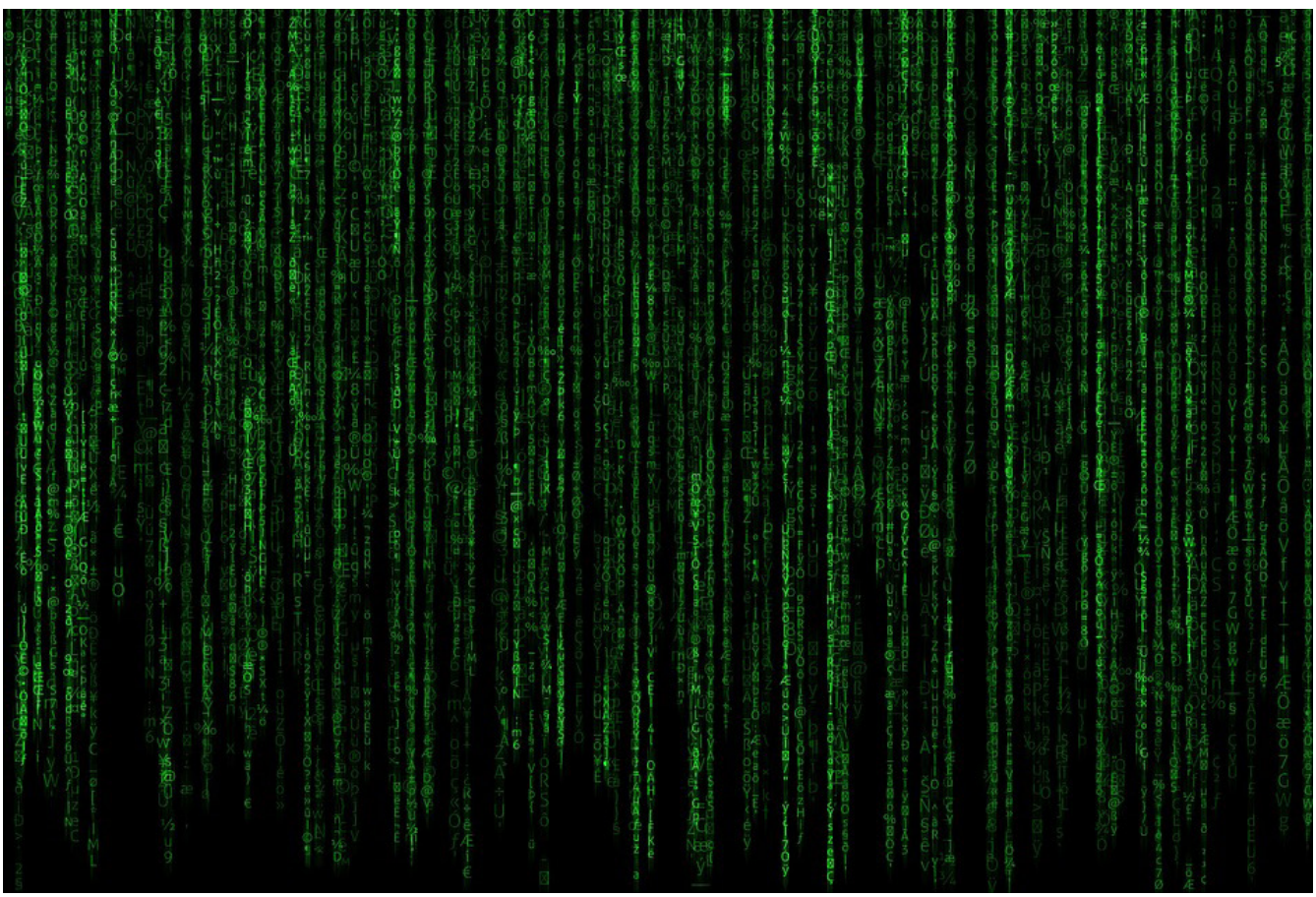
Ролята на киберсигурността се променя в зависимост от еволюцията в световен мащаб. Може да се определи, че киберсигурността е константно явление, което следва еволюционното развитие на човешкото познание, технологиите и е съвкупност от инструменти, правила, политики, концеп-

ции, гарантиращи мерки за сигурност, дейности, обучение, придобит опит от практиката.

Успешното реализиране на целите на киберсигурността и ефективното използване на възможности на притежаваните ресурси (сили и средства) в значителна степен зависи от умело изградената и устойчиво функционираща система за киберсигурност[5].

Актуалността на киберсигурността се предопределя от настъпилите в съвременния дигитален свят глобални промени, които породиха множество противоречия и създадоха комплексно единно цяло от взаимодействащи киберобекти. Нейната значимост се обуславя от експоненциален ръст на генерирането, събирането, анализирането, съхраняването и обмена на информация в резултат на технологични иновации. Бурното развитие на информационните технологии и изграждането на глобални информационни инфраструктури създадоха нови уязвимости, а организациите и обществото станаха обект на множество невиждани досега форми на престъпност.

Независимо от типа на системите за киберсигурност и характера на съставящите ги компоненти (подсистеми, елементи), те притежават единни свойства, по които се различават от



общоприетите съвкупности от обекти, процеси, явления. Най-общо може да се определят тези свойства, като:

уникалност - всяка от системите за киберсигурност няма аналог в поведението си като процес или в състоянието като резултат (или са толкова рядко явление, че тяхното наличие не се взема под внимание в теорията и практиката);

непредсказуемост - изразява се във факта, че никое, колкото и подробно да е, познаване на структурата и функциите на съставните части, не дава основание да се определят еднозначно реакциите или функциите на системите за киберсигурност като цяло. Непредсказуемостта не означава непрогнозируемост. Напротив, вземането на управленско решение по отношение на изграждането и функционирането на системите за киберсигурност следва да се основава на прогнозата за очакваното състояние на системите за киберсигурност и средата към времето за реализация на тези решения. Но тук може да се формулира въпросът, доколко тази прогноза може и е абсолютно точна;

неентропийност - практиките по осигуряване на способността на системите за киберсигурност за даден период от време, в определени граници, да запазва основния процес, за който е създадена, да съхранява известна определеност на своите функции и да недопуска несанкционирани действия от вътрешни и външни случайни въздействия. По смисъл, неентропията е противоположна на понятието „ентропия“, известно от теорията на информацията като мярка за неопределеността на състоянието на дадена система. При това, следва да се има в предвид, че ентропията, като работна категория притежава цифрова стойност, но физически е неизмерима величина. Неентропийността е възможността на системите за киберсигурност да управляват своята ентропия и изпълняват поставените й задачи. Поради притежаваната уникалност и слаба предсказуемост, те са разпознаваеми, защото са създадени от човек, но се подчиняват на определени закономерности;

достъпност (Availability) - системите за киберсигурност предоставят мрежови услуги и следва да бъдат на разположение всеки път, когато те са необходими. Това се гарантира чрез водене на борба с атаки от типа „отказ от услуга” (DoS) и атаки, предизвикващи загуба на енергия (захранване) „енергиен глад”;

безотказност (Non-Repudiation) - системите за киберсигурност предоставят услуги, която предоставя доказателства за целостта и произхода на данните. Тази услуга гарантира, че източникът на съобщението не може да отрече, че го е изпратил. Тя е полезна за откриване и изолиране на компрометирани възли;

целенасоченост - това е свойство на системите за киберсигурност в резултат на дейности, извършвани от потребителите, свързани чрез Интернет;

Всяка система за киберсигурност, функционира с определена цел, за постигането на която се съсредоточават множество материални, енергийни и информационни ресурси в интерес на които са насочени действията на всички съставни компоненти на системата като цяло.

Целенасочеността намира израз в стратегията на система за киберсигурност, която определя поведението в съответствие с динамично изменящите се условия.

Посочените общовалидни свойства и тенденциите за развитието им генерират безпрецедентен дефицит на идеи, концепции и модели за еволюционно развитие и повишават търсенето на нови технологии в съвременния дигитален свят.

Особено актуални днес са новите информационни технологии, които запълват една съществена потребност от високоефективни комуникации, обработка на информация и управление. Ефективността на системите за киберсигурността са необходими не само на държавни институции, а и на ръководителите на големи корпорации, както и на отделни потребители в световната мрежа Интернет.

Киберсигурността се заключава в разработване и прилагане на адекватни на съвременни предизвикателства, нормативна база, „кибер хигиена»(„кибер култура»), основаваща се на придобити знания и умения, опит, взаимосвързани практически действия с цел постигане на киберсигурност при навигиране в мрежата.

Функционални характеристики на системите за киберсигурност.

Успешното решаване на задачите по анализа и определяне на свойствата на системите за киберсигурност, по структура и значение на параметрите и синтеза, по зададени свойства на системите, не е възможно да се извърши само с нестойностна оценка в различни условия на функциониране. Системотехниката изисква количествена оценка на поведението и свойствата на системите за киберсигурност.

Количествените данни за поведението на системата могат да бъдат в пределите на възможното или приближена оценка по експериментални данни.

Ефективност на системите за киберсигурност

Всяка от системите за киберсигурност може да се разглежда като обект, предназначен за изпълнение на определен вид дейности или за решаване на точно определени задачи. При това процеса на функциониране на системите за киберсигурност се представя като съвкупност от действията на нейните елементи в съответствие с поставената цел.

Ефективността на системите за киберсигурност преди всичко се ограничава в определянето на собствената, вътрешна ефективност на системата, под наименованието, на която се разбира степента на приспособеност на системите за киберсигурност към осигуряване потребностите на управлението по обмен и обработка на информация със зададено качество в условията на работа на управляващата система.

Необходимо е конкретно формулиране на задачите и целите на функциониране на системите за киберсигурност, като при правилно определени такива, може да се говори за качество в работата на същите.

Качеството на системите за киберсигурност се оценява, чрез показателя ефективност - или това е числова характеристика, която оценява степента на адаптиране на системата, при изпълнението на поставените пред нея задачи.

Под ефикасност (ако няма друго определение) се разбира съотношението между използваните ресурси и планираните за използване ресурси.

значителен набор от подпоказатели. Обикновено те се съставят от сумирани директни и сумирани индиректни разходи. Друга възможност е използването на показатели включващи разходите по въвеждането на информационните системи () и разходите за управление.

$$R_{ефикасност} = 1 - (\frac{R_{използвани\_ресурси}}{R_{планирани\_за\_използване\_ресурси}})$$

Анонимността на интернет пространството предоставя възможност за извършване на киберпрестъпления, които трудно се проследяват или доказват, но въпреки това, резултатите от функционирането на системите за киберсигурност се изразяват количествено във вид на някаква величина (например - брой заплахи засягащи Web сървърите за 24 часа; измами, фалшифициране и кражба на самоличност;атаки срещу информационни системи, отказ от услуга и имплементиране на зловреден софтуер и т.н.). Трябва да отбележим, че от това каква числова характеристика на системите

$$R_{ефикасност} = 1 - (\frac{R_{разходи\_за\_управление\_с\_ИС} + R_{разходи\_за\_въвеждане\_ИС}}{R_{разходи\_за\_управление}})$$

Икономическата измеримост на двата основни показателя могат да включат за киберсигурност е избрана в качеството на показател за ефективността,

зависят резултатите от нейното изследване.[6]

Надеждност системите за киберсигурност

Надеждността на системите за киберсигурност се характеризира, чрез способността на същите да запазват своето качество за времето на експлоатация. Често това понятие се заменя с понятието техническа надеждност, с което се определя времето за безотказно изпълнение на функцията на определено изделие. Имайки в предвид характеристиката на системите за киберсигурност и определянето им като сложна система, е възможно да се формулира надеждността като вероятност за безотказна работа на системата в хода на целия жизнен цикъл. Надеждността може де се описва с различни вероятностни характеристики – вероятност за безотказна работа в зависимост от времето, параметри на отказите и други. Необходимо е сега да бъдат избрани такива показатели, които характеризират надеждността на системите за киберсигурност като цяло.

Под структурна надеждност на системите за киберсигурност може да се разбира, съвкупната надеждност определена от способността за безотказна работа и способността за функциониране в определени граници под определено несанкционирано въздействие в хода на експлоатацията.

Надеждността като вероятностна характеристика се определя като вероятността $P(t_o)$, състояща се в това, времето за безотказна работа T (случайна величина) да превишава времето на експлоатацията t_o, (константа), което се записва като:

$P(t_o) = P(T>t_o)$.

От анализа на стрктурната надеждност на системите за киберсигурност спрямо оценката на икономическата ефективност на предлаганите варианти за изграждане на системата, е възможно да се вземе управленско решение за определяне на подходяща структура за времето на целия жизнен цикъл на системата.

Качество на управление на системите за киберсигурност

Управлението в системите за киберсигурност играе изключително важна роля, и в тази връзка, оценката на качеството на управлението е една от най-важните страни на общата оценка на ефективността на системите.

В системите за киберсигурност се отделят специални елементи - управляващи устройства, които осигуряват преработка на информацията за целите на управлението. Качеството на управлението в системите за киберсигурност е в пряка зависимост от множество фактори.

Какво разбираме под система за управление на киберсигурността?

Системи за управление

Системи за управление като правило не са просто динамични тех-

нолочични системи, а по-скоро са „натоварени“ с очаквания да решат „нерешими” за управлението задачи. Това в пълна сила важи и за съвременните решения, стъпващи на иновативни научнотехнически разработки. Поради широкообхватната цел се очаква да решават задачи с голяма сложност, а именно:

- поддържане на средства, с които се реализира политиката по киберсигурност на организацията (организационни, технически и др.);
- съвместимост между всички участници в киберсредата;
- обработване на цялата информация достъпна на управляващата система;
- поддържане на ситуационна осведоменост за всички елементи в киберсредата;
- подпомагане вземането на решение от управляващата система;
- поддържане на архив на наличните информационни активи и проведени дейности в организацията.[7]

Удовлетворяването на високите изисквания в практиката към системите за управление се постига чрез интеграция на различните системи, включваща преди всичко архитектурен подход в планирането и изграждането на адекватна, съответстваща на конкретни изисквания комуникационно-информационна система.

Правилата на взаимодействие се определят от функционалната взаимовръзка между елементите, която обикновено е определена под формата на доктрини, процедури или процеси.[8]

Рамките на взаимодействие в системата най-общо се описват в стандарти и технологии.

Системите за управление са добре познати в бизнес организациите. Основните теоретични постановки в областта са систематизирани през XX век, и се реализират въз основа на съвременни технологии като експертни системи, системи за групово вземане на решение, системи с изкуствен интелект и други, познати още като „интелектуални инструментални системи”, подпомагащи процеса за вземане на решение. Текущото имплентиране на идентични системи в сферата за киберсигурността е естествен процес, отчитайки общите изисквания към процесите за вземане на управленски решения. Общото в процесите за вземане на решение в бизнеса и системите за киберсигурност е тяхното реализиране в среда с висока степен на неопределеност.[9]

Устойчивост на системите за киберсигурност

Качеството на функциониране на системите за киберсигурност, може да се оценяват с помощта на набора от числови характеристики, като ефективност, надеждност и т.н., изчислени за зададени условия на функциониране на системата. От тази гледна точка, системата само тогава притежава ис-

каните свойства, когато избраните характеристики се намират в зададени предели или принадлежат на някоя област.

Условията на функциониране на системите за киберсигурност се различават от нормалните и за това е важно да се знае, съхраняват ли се свойствата на системата при наличие на смущения. На тази почва възниква понятието устойчивост на функциониране на системите за киберсигурност.

Под устойчивост на функциониране на системите за киберсигурност се разбира, способността на системата да съхранява основните си свойства в условия на действия на несанкциониран достъп. За да бъде това понятие по-точно е необходимо да се определи вида му, да се опишат разглежданите свойства на системата. Понятието устойчивост се отнася не към системите за киберсигурност, а към някое свойство на функционирането й. То се явява определящ фактор при избор на способа за измерване на различията между процес на функциониране на системата, без и с несанкциониран достъп.[10]

В заключение може да се обобщи, че навлизането на съвременни технологии във всички направления в

световен мащаб ще продължи в дългосрочен аспект. Този факт ще наложи трансформиране, разширяване и уплътняване на киберпространството, чрез виртуализиране на все по-широк спектър от услуги. В този контекст могат да се очакват все по-многобройни и сложни заплахи за националния и международен сегмент в киберпространството, които водят до асиметричност в последиците.

Постигането на киберсигурно и киберустойчиво общество ще зависи от политическата подкрепа, ресурсното осигуряване, степента на сътрудничество на ведомствено, регионално и международно ниво.

Това може да се реализира с прилагане на спираловиден подход в три направления: изготвяне/актуализиране на политики, изграждане/модифициране на структури и създаване на капацитет за провеждане на стандартизирана подготовка на експерти.

(Endnotes)

1 Иванов, Г. Концептуални аспекти на киберсигурността, Сборник научни трудове ISBN 978-954-9681, Шумен, 2014, с. 266 -271.

2 Иванов, Г. Аспекти на киберсигурността, Международна конференция „Хемус-2014", ISSN 1312-2916, с. II-106 do II-112.

3 Димов, П. Приложение на уеб технологии за защита на националната сигурност, ISBN 978-954-2977-47-6, Диомира, 2018

4 Чакъров, И. Киберсигурността – част от мениджмънта, списание CIO, 2017, ISSN 1312-5605.

5 Симеонов, Т. Аспекти на усъвършенстването на подготовката на офицерите за осигуряване с информация на многонационални щабове в операциите, различни от война, Конференция на факултет „Командно-щабен", 2006 г., ISSN 1312-2991.

6 Chakarov, I., SocioBrains – Intenational Scientific Refereed Online Jornal–2017, Cyber resilience–basic aspects in the security sector, Issue 32, April 2017.

7 Chakarov, I., NRDC-GR Herald Magazine, Issue № 8, 2016-2017, Cyber security as part of the contemporary security environement.

8 Калчев, К. Цветков, К. Киберсигурност, Военна академия ЮГ. С. Раковски", 2018.

9 Пак там

10 Chakarov, I., SocioBrains – Intenational Scientific Refereed Online Jornal–2017, Cyber resilience–basic aspects in the security sector, Issue 32, April 2017.

Информационните операции и не насилствените революции

Автор: Подполковник д-р Живко Желев

INFORMATION OPERATIONS AND NON-VIOLENT REVOLUTIONS
Zhivko Zhelev

***Анотация**: Статията представя анализ на възможностите за използването на информационните операции при провеждането на дейности при не насилствените революции. Представеният в статията модел за прилагане на информационно въздействие върху целевите групи е съществен за постигане на успех в подобни начинания.*
***Ключови думи:** информационни операции, не насилствени революции, информационно въздействие*

***Annotation:** The article presents an analysis of the possibilities for the use of information operations in conducting activities in non-violent revolutions. The model presented in the article for implementing information impact on the target groups is essential for success in such initiatives.*
***Key words**: Information Operation, Non-violent revolutions, Information impact*

Информационните операции са заели изключително важно място в съвременните конфликти. Тяхната приложимост има решаващо значение за снижаване на разходите, времето, бойните и съпътстващите загуби при провеждането на съвместни операции. Не без значение са и превантивните им функции по възпиране от потенциални действия срещу заплахи за сигурността на страната.
Провеждането на информационните операции е повлияно не само от характера на информационната среда и способностите за провеждането им,

но и от вида на операциите, които се провеждат. Целите, задачите, средствата и подходите за провеждането им ще са различни и уникални, за да отговорят на предизвикателството на средата и да осигурят надеждна и ефективна подкрепа на съвместните действия за постигане на поставените цели. Комбинирането им с технологии като например тези на гражданско-военни операции и сътрудничество с „подкрепяща функция, които да са в непрекъсната ангажираност с всички части на населението на страната, за усъвършенстване на уменията за ориентиране в такава ситуация, както и националната ангажираност и устойчивост“[1] е наложително и дори задължително.

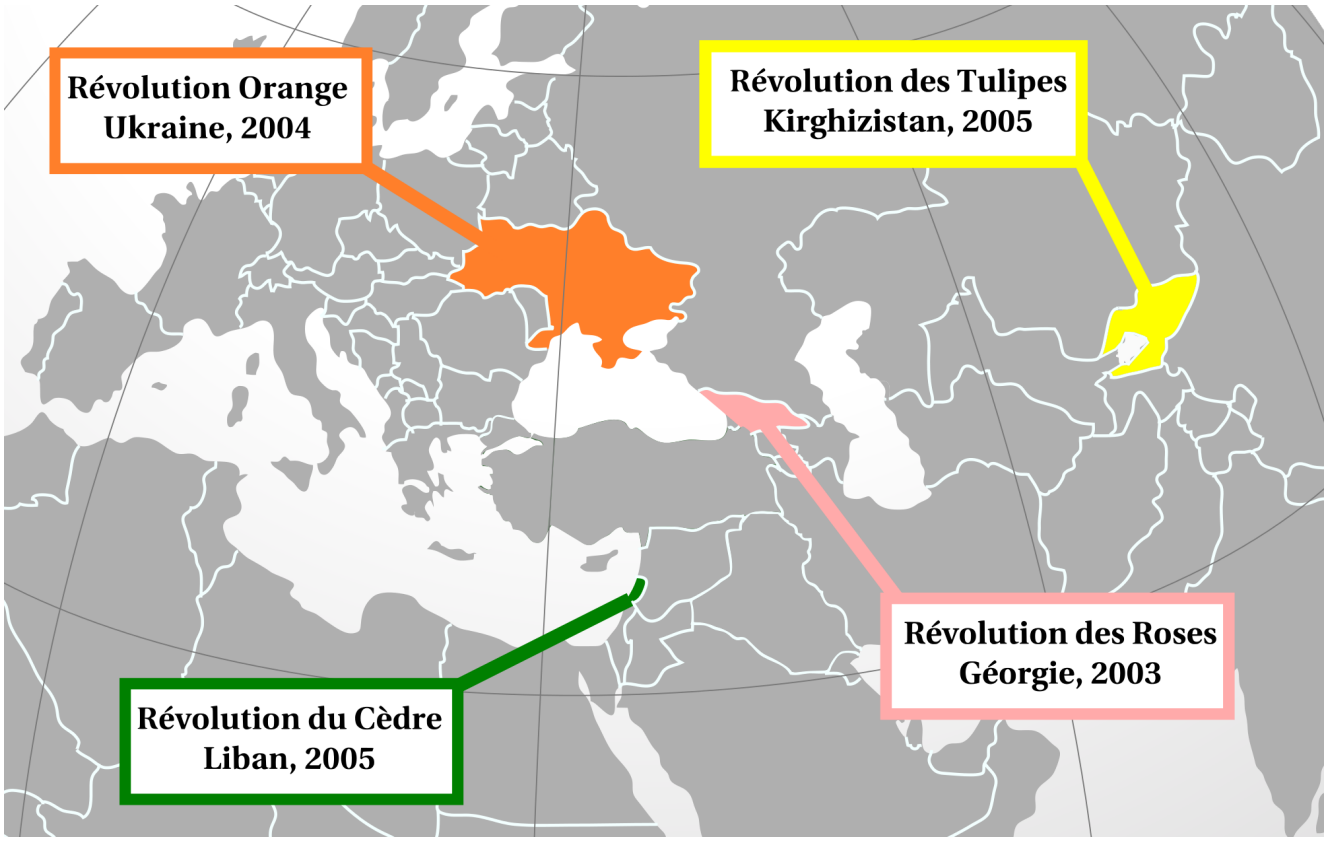
През втората половина на 20-ти век отделни черти на не насилствената смяна на властта, по известни като „нежни” и „цветни” революции се забелязваха в редица страни. Но макар и близки по значение двете понятия носят и съществени смислови различия.

„Нежната” революция представлява смяна на властта с не насилствени средства с умерено използване на външна за страната подкрепа (предимно финансова и морална подкрепа), при която се извършва кардинална смяна на управляващия елит и политическата система.

При ***„цветните” революции*** не се наблюдава смяна на обществения строй, а движението на елита има ограничен характер, тъй като властта преминава от една управленска група към друга управленска група (кръг от доминиращи политически и икономически субекти). Поради тази причина в държавата настъпват само частични промени в политическата система.

При втория вид революции е необходимо да се отбележи, че външната подкрепа е значително по осезаема и може да включва действия по обединяване на опозиционните партии, значително финансово подпомагане, издигане на авторитета на един от опозиционните лидери за участие в предстоящите избори, оказване на морална и политическа поддръжка на опозицията от страна на световната общност, създаване и финансиране на младежки организации, чиято роля е провеждането на масови акции на „не насилствена съпротива” на официалната власт и представяне на народния протест, организиране на паралелно преброяване на гласовете при провеждането на избори с цел обвиняване на властта в тяхната манипулация и подтикване на обществото към масови протести.

Освен това при „цветните” революции се наблюдава и явна промяна на външно политическия курс на страната. Следователно основното различие между „цветните” и „нежните” революции е ролята на външната за страната сила, която подпомага финансирането, подготовката и смяната



на властта в страната.

Технологията за подготовка и провеждане на „цветни" и „нежни" революции е така изградена, че максимално да се прикрие външната подкрепа, която явно следва своите дългосрочни интереси. За тази цел се използват международни правителствени и най-вече неправителствени организации, за обезпечаване на идеологическата, финансовата и организационната подготовка[2].

Създателят на теорията за не насилствената сляна на властта, лежаща в основата на „цветните" и „нежните" революции е Джин Шарп (Gene Sharp), научен ръководител на Алберт Айнщайн институт (AEI) оглавяван от бившия ръководител на разузнавателното управление на Министерството на отбраната на САЩ полковник в оставка Роберт Хелви (Robert Helvey).

През 1993 г. Шарп публикува книгата ***„От диктатура към демокрация. Концептуални основи на освобождението"***, която се превръща в основно учебно пособие на активистите на „цветните" и „нежните" революции. Специално разработените методи включват широк спектър от не насилствени действия, като разобличаване на властта (информационна война срещу действащата власт), масова кампания по разобличаване на законността на действащата власт, лишаване на действащата admini-

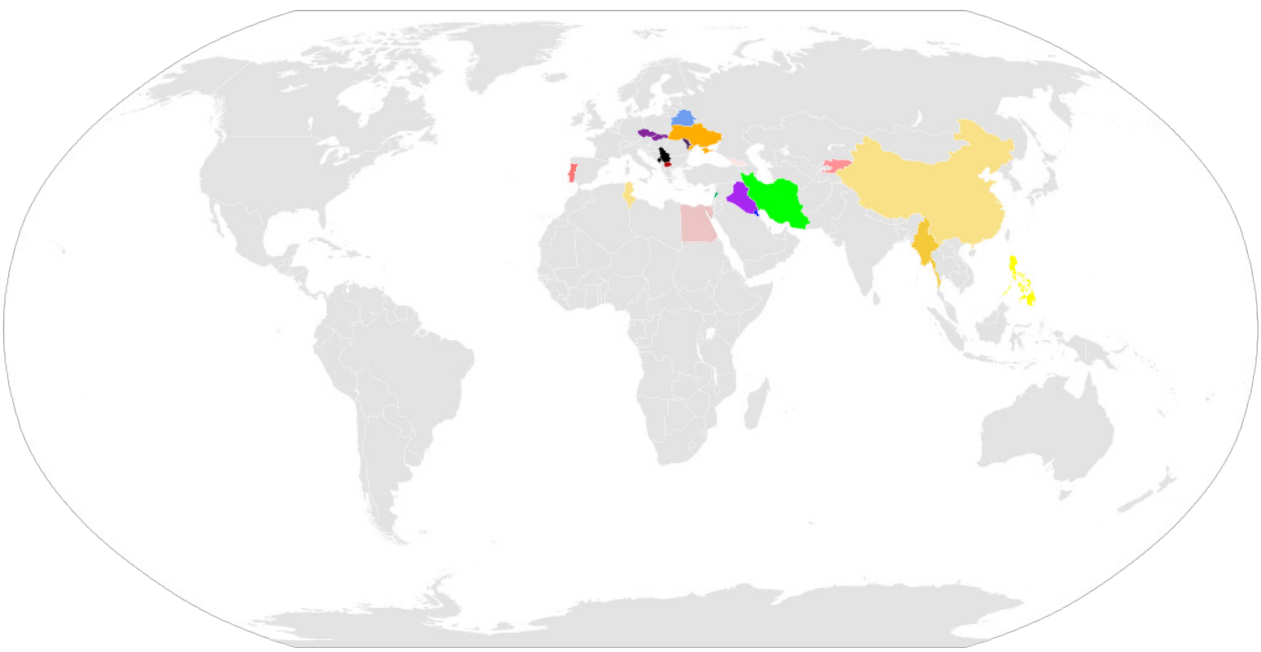
страция от възможност за изпълнение на своите задължения и правомощия посредством не насилствена съпротива, активна разяснителна работа със служителите от администрацията от различните нива, действия по „разлагане" на армията и силовите структури в държавата, създаване на ситуация на двувластие в страната, поставяне под контрол на транспорта, снабдяването, обществените комуникации, медиите и др.

Реална опора на действията на опозицията при активното противопоставяне на действащата власт са най-неустойчивите в идеологическо отношение слоеве от обществото – младото поколение и недоволните от властта либерално настроени части от интелигенцията[3].

Ако се направи анализ на „цветните" и „нежните" революции от последните две десетилетия, може да се достигне до извода, че те протичат по един и същи сценарии при следната ***технологична схема***:

Подготвителен етап (до началото на предизборната кампания). Това е най-продължителният етап свързан със създаване, обединяване и активизиране на вътрешната опозиция. Основната задача е да се сплотят опозиционните партии около един кандидат, завоюване на популярност след най-уязвимите слоеве от обществото (младежи и интелигенция), създаване на младежки организации, като движеща сила на бъдещата революция представяйки се като „целия" народ и привличане на своя страна ръководствата на болшинството от националните медии.

На този подготвителен етап се извършва постепенно и целенасочено



отслабване на властта, чрез използване на нейните вътрешни слабости. Основните дейности са:
- обединяване на опозицията около един кандидат;
- определяне на райони от страната, където опозицията ще се ползва с гарантирана подкрепа на избирателите;
- създаване на младежка организация и подготовка на нейните лидери и активисти за не насилствени протестни действия, управление на голяма маса от хора и към пасивно съпротивление на право охранителните органи при провеждането на масови мероприятия;
- осъществяване на явни и прикрити подкупи на ръководствата на болшинството от националните медии за провеждане на активна кампания за създаване на положителен имидж на кандидата на опозицията и планомерна и все по твърда критика към правителството на страната и към кандидата на управляващите в предстоящата предизборна кампания;
- осигуряване на постоянно и целенасочено подриване на лоялността към държавата посредством привличането към сътрудничество на отделни лица от висшия команден състав на силовите структури. Това трябва да доведе до неутрализация на сектора за сигурност (специални служби, полиция и армия);
- оказване на финансова и материална поддръжка на опозицията и нейните лидери, материално осигуряване на процеса на подготовка на опозицията и провеждане на активна работа с етнически и културни малцинства и „колебаещи" се групи посредством международни неправителствени организации, посолства, консулства, търговски представителства и др.;
2. *Междинен етап (от началото на предизборната кампания до провеждането на изборите).* Този етап се характеризира с увеличаване на количеството на антиправителствени прояви, масови прояви, протести, представяне на дейността на различни комисии, работни групи и организации за представяне на злоупотребите на длъжностните лица със служебното им положение и управленската им слабост. През този междинен етап медии е необходимо да:
- представят подготовката за изборите, компрометирана от управляващите и подготовката за манипулиране на резултатите от управляващите. За целта е добре да се използват както национални така и международни медии предварително подготвени за участие в подобни действия;
- за изборите се привличат колкото е възможно повече наблюдатели, от страни близки до оказващата външна финансова подкрепа, които трябва да изпълнят две основни задачи: да потвърдят фактите на масови нарушения на демократичните норми в предсрочните избори и придаване на

легитимност на разнообразни проучвания на общественото мнение, които могат да се използват срещу управляващите при обявяване на резултатите от изборите;
- посредством медиите се оказва въздействие върху управляващите, че само победата на опозицията ще е свидетелство за демократичността на изборите;
- в столицата и в големите градове се провеждат масови мероприятия, прерастващи в безсрочни, които намират обширно отразяване в приближените до опозицията медии;
- в опозиционните медии и интернет в реално време се публикуват резултата от проучвания на общественото мнение и от международни наблюдатели демонстриращи „убедителната победа" на опозицията;
- до официалното обявяване на резултатите от изборите опозицията заявява своята победа. Ако официалните предварителни резултати се окажат в полза на управляващите, то незабавно се обявява, че изборите са „фалшифицирани";
- под ръководството на лидерите на опозицията на опозиционни депутати, ползващи се с имунитет, се блокират или не насилствено се завземат правителствени и административни здания и пълно или частично се блокира дейността им;
- оказване на дипломатически[4] и медиен натиск върху ръководството на страната за не използване на сила срещу протестиращите.

3. *След идването на власт на опозицията се извършва:*
- промяна в съотношението на административно-финансовите групи в страната изразяващи се в преразпределение на финансовите потоци.
- извършва се промяна на външно политическия курс;

От всичко посочено до тук можем да изведем характерните черти на „цветните" и „нежните" революции:
- наличие на стандартен подход за провеждането им;
- представяне на определени направления от обществено-политическия живот в страната и изразена външна подкрепа за опозицията;
- използване на механизма на „меката сила";
- ясно изразена външна насоченост на влиянието на политическите процеси в страната;
- основната цел е завземане на властта.

Една от основните причини, поради която „цветните" и „нежните" революции имат успех е контролът на информацията или как информацията се контролира сред протестиращите. За тази цел широко се използва пропагандата в хода на провеждането им. Тя е изключително ефективна като форма на емоционално общуване, а не като форма на критическо мислене[5]. Целта е налагане на определено пове-

дение, което подтиква хората да излязат на улицата и да отслабят позициите на управляващите.

От представеният модел за провеждане на подобни не насилствени революции проличават няколко основни направления за информационни дейности, в които информационните операции ще имат решаващо значение, а те са:

контрол на информационната инфраструктура;

привличане и контрол над водещи медии специалисти (собственици или административни ръководители на медии, програмни директори, водещи журналисти, редактори и др.);

създаване на програмни продукти и интерес на провежданите от опозицията действие.

Тези представени действия осигуряват посланията на опозиционните лидери да се разпространяват до възможно най-голяма аудитория, което трябва да осигури широка подкрепа, а следователно и легитимност на изборния процес и новосформираното правителство. Ключов момент е изготвяне на информационни продукти (предавания, репортажи, статии, листовки и др.), в които се дискредитират управляващите. За изготвянето на подобни продукти е необходима специална подготовка, тъй като са необходими специализирани познания в областта на психологическите операции, представяне, поза, профил, операции в мрежите и операции по сигурността. Също така е необходима координация между действия на опозиционните лидери, представяните послания и критичните оценки. Без липсата на подобен синхрон, лесно опозиционните лидери могат да изпаднат в неловки ситуации, собствени противоречия, объркване, обвинения в разпространение на лъжлива информация и пр. Всички тези действия трябва да формират правдоподобна картина на обстановка в страната, да предложат алтернатива или визия за излизане на страната от настоящата ситуация и не на последно място емоционално да подтикват гражданите да гласуват в деня на изборите в подкрепа на опозиционните движения.

Анализирайки тези действия в информационната среда можем да достигнем до извода че това е информационна операция, провеждана в интерес на опозиционните сили и имаща за цел дискредитиране на настоящата власт в страната и осигуряване на национална и международна подкрепа при провеждането на изборния процес и прехода към ново управление на страната. За провеждането на подобна операция като минимум е необходимо да се изпълнят следните условия:

наличие на специалисти в областта на информационните операции, структура и финансиране. Провеждането на подобни операции не е по силите на която и да е политическа партия,

още повече прохождаща. За тази цел е удачно да се използват специалисти в областта които имат необходимите знания, умения и опит в структури занимаващи се с планирането и провеждането на информационни операции. Не е за подценяване и факта че подобни революции без външна подкрепа са обречени на неуспех, а една от основните им задачи е не само смяна на властта но и на политическия курс на страната. Или казано на жаргон това е „превземане на крепостта от вътре".

наличие на подходяща информационна среда. Това е необходимо за да се осигурят канали за връзка между опозиционните лидери и целевите аудитории. Въпросните канали не са нищо повече от класически и нови медии. Чрез тях ще се предават посланията или продуктите на информационното въздействие, за да се спечели подкрепата на населението. Това е възможно да се случи при отвореното информационна среда в която има свобода на медиите или при загуба (отказ) на контрол от страна на правителството. Следователно, контролираната и затворената информационна среда са неблагоприятни и затрудняват провеждането на подобни операции. Дори в затворената информационна среда подобни операции са напълно невъзможни.

наличие на „продукт" който да бъде представен. Като формален продукт на подобни въздействия се явяват всички онези информационни материали разпространявани планово и координирано за осигуряване на подкрепа от местното население. Но неформалният продукт е новата идея за развитието на страната, новата визия на управляващите и лица в политическия елит. Това е новата марка (бранд) в управлението на страната. И в тази ситуация хората ще се интересуват от същите проблеми както при контра бунтовническите операции: кой ще е новият управляващ и ще им осигурили необходимата сигурност. [6] Следователно представянето на марката (бранда) ще е ключова за успеха на подобна операция, за нейното възприемане и успешното провеждане на изборния процес.

Един от известните технически приоми на пропагандата, който се използва за свалянето на нежелани лидери е „брандинга" (създаване на марка). По своята същност пропагандистите се опитват да подсилят „бранда" на опозиционните лидери и движения и да отслабят „бранда" на целевия лидер или система. Те рядко говорят за конкретни проблеми на обществото или решения. Вместо това те се насочват към представяне на „бранда" и свързаните с него въпроси посредством широко използвани емоционални термини. Опозиционните движения се описват с изрази като „весел", „патриотично", „честно", „справедливо", „революционно" и прочие,

докато проблемите на обществото се задълбочават и се насочват към определени схеми с корупционен, приватизационен и монополен характер, покровителствани от „жадни за власт" политически фигури. Целта на подобен тип съобщения е да са лесно възприемани от обществото, да повярват хората в предлаганата от тях истина. По същество политическите послания са скучни и безинтересни, което налага необходимостта тази политиката и политическите послания да се представят привлекателно, да придобият вид на модно течение привличащо последователи. Това е „брандинг" логиката, която се използва за постигане на вътрешно политическо съгласие и за оправдаване на външно политическите дейности.

Ако погледнем проблема с представянето на „бранда" от противостоящата страна, от гледна точка на управляващите то единствения разумен подход за защита от тази логика на този метод е да се предизвика отказване от „бранда". За тази цел опозиционните медии никога не трябва да се ограничават или забраняват. Вместо това трябва да се подпомогнат собствените или поддържащи медии с инструменти за ефективно противопоставяне. Правителството трябва да стане спонсор на нови и по-модерни средства за масова информация. Да подпомага неговите програми, поставянето на културни и образователни предавания, с което медията да спечели и да поддържа висока популярност сред местното население. Предаванията трябва да са увлекателни, съдържателни, основаващи се на традиционните национални и религиозни добродетели, но и да се представя и съдържателна критика. Тези проправителствени медии трябва да се използват, за да се разруши „бранда" на опозиционните сили и да се замести с нов алтернативен и успешен „бранд". Идеята се заключава в това, че е по-добре да се привлекат младите хора на своя страна, отколкото да се арестуват. Да се привлекат в управлението личности ползващи се с доверие и способни да работят с младите и енергични хора. В подобни ситуации любовта към отечеството не е достатъчна, ако не е обвързана с доверие към правителството. Най-ефективният способ за привличането на младите хора към участие в разрешаването на проблемите на страната е посредством създаване, на усещането, че те са реална част от властта и управлението. В противен случай тези хора се лутат между различните идеи и цели и могат лесно да бъдат привлечени в „противостоящият лагер".

За подсилване на собствения „бранд" могат, да се използват и чужди международни медии, чиято дейност може да се насочи в посока на разкриване на дезинформацията и представяне на собствената позиция зад граница. Това в значителна степен намалява

влиянието на чуждото информационно[7] въздействие, гарантира възможността за защита на националните интереси в дългосрочен план и запазване на инициативата в борбата за информационно превъзходство над широките обществени маси. Смисълът на тези действия се заключава в укрепване на контактите и сътрудничеството с независимите медии, които ще подпомагат създаването на обективна и балансирана картина на обстановката в страната, посредством представяне на критични репортажи и културен обмен, свободен достъп до административна информация и значими политически, културни и др. личности. Това е помощ, която ще подпомага изграждането на собствения „бранд".

Следователно изграждането на привлекателен „бранд" в съчетание с подходящо представяне са ключова предпоставка за успех при провеждане на ненасилствени революции и за опозиционните сили и за управляващите. Това е възможно посредством провеждането на детайлно планирано и координирано информационно въздействие осигуряващо необходимата обществена подкрепа за законно управление на страната.

Обобщавайки използването на информационните операции в съвременните конфликти и кризи може да се направи заключение, че при тяхното прилагане се следва определен логически модел, позволяващ постигането на поставените цели на информационното въздействие. Този модел смело можем да кажем, че ще бъде модифициран в различните условия и ще може да се прилага в различен обем - съобразно характера на кризата, произтичащите ограничения от информационната среда, противостоящите сили в едно информационно противоборство, но основните му фази могат да се представят в следния вид:

Набиране и подготовка на специалисти и информационни агенти за провеждане на информационна операция.

Получаване на достъп и контрол до информационна инфраструктура необходима за провеждането на информационните дейности.

Формулиране на история, теми, целеви групи и канали за информационно въздействие.

Валидизиране на подготовката за провеждане на активни информационни дейности.

Провеждане на активни информационни дейности (граждански и военни) за формиране на обществени нагласи и заблуда на военното и държавно ръководство на противостоящите сили, относно провежданите действия от собствените сили (поддръжници).

Представяне и поддръжка на постигнатите резултати пред местната и световна общественост.

Този модел е приложим както при

кризи и конфликти с използване на военна сила, така и при вътрешно държавни кризи без използването на военна сила, дори и при продължително водене на информационна война. Той позволява цялостно използване на информацията, като елемент на националната и военна мощ и способства за снижаване на разходите и загубите при евентуално активно въздействие и от противостоящата страна.

Следователно, при извършване на не насилствена дейности за смяна на властта, информацията се явява основен инструмент за въздействие, посредством които се оказва влияние, както върху избирателите, така и върху международната общественост. В подобни дейности се използват всички познати и непознати манипулативни технологии за информационно въздействие, а контролът над информационната инфраструктура и нейното нормално функциониране са от решаващо значение за изхода от подобни обществено значими дейности.

(Endnotes)

1 Кисьов, М. Новите предизвикателства и подхода на функцията и способността „Гражданско-военно сътрудничество“, Българска наука, 2019

2 Кузьмин В., Роль США в осуществлении «цветных революций» в зарубежных странах, http://pentagonus.ru/publ/19-1-0-822 (15:00 ч. 18.05.2016)

3 Gene Sharp, From Dictatorship to Democracy - A Conceptual Framework for Liberation, 2010, p. 2 – 8

4 Ivanov, G., Podgotovka, otgovornosti, funktsii i zadachi na voenniya atashe //Spisanie „Voenen zhurnal“ br.1, 2014, ISSN 0861-7392, s. 130-131.

5 Львович Иг., Глобальные информационные войны 21-го века или как избежать «цветной» революции, 2012, http://perevodika.ru/articles/20749.html (15:00 ч. 26.05.2016)

6 Стойчев, С., Изследване способностите на НАТО и ЕС за отговор и управление на кризи, Военна академия, 2015, монография, ISBN 978–954–9348–62–0, стр. 135

7 Иванов, Г. Аспекти на киберсигурността, Международна научна конференция „Хемус -2014”, ISSN 1312-2916, Пловдив, с. II-106 до II-112.

Перспективи и възможности за усъвършенстване на частните услуги за сигурност в България

Автор: Татяна Иванова

Анотация: През последното десетилетие бизнеса на частните услуги за сигурност макар и не признат в целостта му в България става все по-професионален в резултат и на членството ни в ЕС и на стремежа на сектора за доставяне на висококачествена услуга. Зачитайки важната роля на частните услуги за сигурност в днешното общество, може да бъде само в интерес на обществото като цяло, да се намерят адекватни решения за ограничаване на загубите, "навлечени" върху всички търговски страни в тази индустрия до приемливи нива и/или нива които да осигуряват алтернативни финансови източници за покриване на загубите. Очевидно е също, че за да се намери дългосрочно решение на въпросите за критичната отговорност, резултат от терористични атаки или военни действия, е нужна някаква форма на ясна правна рамка в ЕС, респективно и в България за различните сектори.

OUTLOOK AND OPPORTUNITIES FOR IMPROVEMENT OF PRIVATE SECURITY SERVICES IN BULGARIA

Author: Tatyana M. Ivanova

Annotation: Over the last decade, the private security business, although not recognized in its integrity in Bulgaria, is becoming more and more professional as a result of our EU membership and the sector's drive to deliver high-quality service. Considering the important role of private security services in today's society, it may only be in the interest of society as a whole to find adequate solutions to limit the losses attributable to all trading parties in this industry to acceptable levels and / or levels which provide alternative financial sources to cover losses. It is also obvious that in order to find a long-term solution to the issues of critical responsibility, caused by terrorist attacks or military action, some

form of clear legal framework in the EU or Bulgaria is needed for different sectors.

Key words: private security services, security sector reform, Bulgaria legislation, possibilities for improving;road map

В действителност специфичната природа на частните услуги за сигурност, тясно свързани с основните въпроси на сигурността в обществото, изисква установяването на строги условия, специфични за сектора, по-специално за влизането на пазара, проучването на служителите в заети в сектора на частните услуги за сигурност, обучението, определянето на дейностите и правото и задължението за националните власти да осъществяват постоянен контрол върху частните фирми за сигурност.

Европейските страни поемат по-активна, по-отговорна и по-глобална роля за посрещане на съвременните рискове и заплахи за сигурността, включително и такива във вътрешен план. Европейският съюз се стреми да намери решение на разнообразните рискове и заплахи чрез гъвкави, ефективни и законни решения.[1] В тази посока можем да посочим, че се усилията за европейска хармонизация на сектора на частните услуги за сигурност. Същата винаги е играла ключова роля във всички съвместни дейности и проекти касаещи сигурността на страните-членки, но цялостната европейска хармонизация в сектора на частните услуги трябва да бъде планирана като постъпателно развитие.

Някои европейски държави имат вече детайлно развито и с високо качество законодателство. Именно тези разновидности на нормативната уредба и регулиране трябва да служат като основа за каквато и да е бъдеща европейска хармонизация, за да се повишава общото ниво на нашата индустрия. Има много конкретни причини да се подкрепя и развива постъпателно хармонизацията.

Национални правила понякога не съществуват, не са адекватни и не гарантират професионализма, от който секторът се нуждае. Те отличават една държава от друга и пречат на сектора да извлече пълната полза от европейската интеграция.До преди няколко години термина „частни услуги за сигурност“ почти не се използваше в бизнес отношенията, да не говорим за комплексна услуга или за бранш. В повечето случай в него се влага другото определение на частната охранителна дейност.В началото на 90-те години охранителната дейност не е регулирана и от това възникват проблеми, характерни и за други сектори, което се дължи и на наследството от централизирания характер на предходния политически строй и неговите регулации. По това време

някои охранителни фирми са пряко свързани с организирани престъпни групи, а в някои случаи и с крайни силови и демонстрационни политики. За другите дейности от обхвата на сектора много малко се говори или въобще не се споменават като елемент от този сектор.Сред тях са и: консултантите по сигурността, проектирането и изграждането на системи за сигурност, видеонаблюдение, пожароизвестяване и пожарогасене, детективите, мониторинг центровете.Във времето тези услуги са разпръснати в различни сектори на икономиката, както в България така и в по голямата част от страните членки.

Това противоречие, както и факта че сектора се развива и разраства на технологично и бизнес ниво с много бързи темпове, а регулаторната политика и бизнес изискванията към него изостават като цяло, ни помагат да посочим актуалността на проблема, а именно: необходима е реформа в сектора на частните услуги за сигурността, чрез която да се усъвършенстването и да се посочи пътя за неговото развитие напред в национален мащаб.

Пътна карта за развитие на сектора на частните услуги за сигурност

Основни параметри

Настоящият документ представлява Пътна карта, която включва ключови проблеми мерките и дейностите за изпълнение на реформата в сектора на частните услуги за сигурност, както и основните участници в процеса, отговорните институции и необходимите мерки и дейности.

За да се постигнат целите в заложени в настоящата пътна карта е направен преглед и анализ в следните ключови области:

Съществуващата на ниво ЕС и Република България нормативната уредба, регулираща развитието на сектора на частните услуги за сигурност;

Съществуващите на ниво ЕС и Република България стратегически документи, които представляват стратегическата рамка за развитието на сектора на частните услуги за сигурност;

Текущо състояние на сектора в Република България;

Проекти, които текущо се реализират или са планирани за реализация в тази област.

На основа на този преглед беше направен първоначален анализ на техническите възможности и характеристики на текущата реализация, за да може да се прецени готовността за бъдещи реализации. По този начин беше определено нивото на съответствие на редица планирани или реализирани инициативи, както от гледна точка задълженията, произтичащи от членството ни в ЕС, така и във връзка с цялостното развитие на сектора и неговото място в икономиката на страната ни.

Стратегическа пътна карта е визуализация на действията, които са необходими, за да се реализират дългосрочните цели за сектора и неговото развитие плавно без сътресения и с високо ниво на успех. Тя идентифицира големите пропуски между текущото състояние и желаното бъдеще и определя и предлага методи и начини за коригиране на тези пропуски.

Добре разработената стратегическа пътна карта е като GPS, който дава информация за сектора и бизнес услугите които доставя. Тя не само показва къде се намираме във всеки един момент, но и кой е най-бързият начин да стигнем до мястото, където искаме да бъдем, с възможно най малко грешки. Образно казано, това е един от най-добрите инструменти за „вдигане на мъглата“ и стратегическо планиране на пътя до целта. Тя ни показва как изборът, който ще направим днес, ще се отрази на нашето бъдеще.

Ефективната пътна карта е насочена към визията, действията и постигане на целите. Щом се уточни визията, това ни води към разработката на пълна пътна карта, която ще включва всички стъпки по маршрута за реформата в сектора на частните услуги за сигурност. Това са целите, които ще ни помогнат да постигнем визията за бъдещето, и необходимите действия, за да бъдат реализирани тези цели.

Основните точки на пътната карта са няколко и изискват от нас да определим:

1) Визия:Ясната визия е важен ръководен стратегически инструмент, който дава дефинирането на сектора, какви задачи, функции и цели има;

2) Принципи и ценности: Принципи и ценности означават нашата „стойност“. Как принципите и ценностите съответстват на визията? Ако те не са съгласувани, какви промени трябва да направим, за да гарантираме, че те ще се възприемат и ще бъдат основата на изграждането и развитието на сектора?

3) Критичните цели: Критичните цели са целите, без постигането на които не можем да предприемем стъпки за да се превърне визията в реалност. За да обхващат сектора като цяло те трябва да присъстват в пътната карта на всяка една дейност от сектора и всяко едно дружество – независимо от подсектора в който функционира.

4) Стратегиите: Това са различните стратегии за постигане на общите цели: ресурсна, потребителска, вътрешно-организационна, учене и растеж.

5) Тактика:Включва всички ключови действия или тактики по всяка една от стратегиите. Това е важна част от пътната карта. Тя прави всеки компонент на картата реалност. Затова в нея трябва да присъстват всички действия, които са необходими, изпълними и измерими - кой какво ще направи и

кога? Стратегиите често се провалят, защото не е отделено достатъчно внимание на тази част.

6) Потенциалните препятствия (SWOT анализ): В пътната карта трябва да бъдат описани всички потенциалните рискове (препятствия) пред всяка една от четирите стратегии,силните и слаите страни – ресурсна, потребителска, вътрешно-организационна и обучение, както и действията, които могат да се предприемат за тяхното преодоляване.

7) Край на етапите (километражни камъни): Това са малки флагове (километражни камъни), които отбелязват местата, където приключват важните етапи от пътя за постигане на крайната цел.

Те са важни както за фирмите от сектора, особено при по-дългосрочни цели, при които е по-лесно да се обезкуражат и предадат, така и за институциите, които трябва да работят принципно и последователно да създават и следват ясни политики и нормативни актове. Краят на етапа дава възможност на ръководителите не само да проследяват напредъка, но и да го анализират със своя екип и да съблюдават за приемствеността

SWOT Анализ на сектора на Европейско ниво

СИЛНИ СТРАНИ

• Европа е **дом на водещите световни частни компании в сектора** на частните услуги за сигурност.

• **Професионализацията**: значителни инвестиции на частните услуги за сигурност - Фирмите са инвестирали значително количество усилия в разработването на схеми за качество и програми за обучение с цел повишаване на качеството на услугите за сигурност

СЛАБИ СТРАНИ

• **Фрагментация** на пазара на Секторът на частните услуги в ЕС произтичаща от различните национални подходи, законодателство и регулаторни среди за услугите за сигурност.

• **Разпокъсаността** също така предполага, че качеството на предоставяните услуги и оперативните разходи могат да се различават значително в отделните държави-членки.

• **Ниски нива на заплатите** и често нерегламентираното заплащане както и лошите условия на труд.

ПРЕДИЗВИКАТЕЛСТВА

• **Готовност на клиентите** да си да платят цена, която отразява на качеството на услугата и подходящо възнаграждение, отразяваща условията на труд на персонала по сигурността. ***Икономическите условия***: повишен натиск за спестяване на разходи по предоставяне на услугата.

• **Условия за възлагане на поръчки:** насърчаване на лоялната конкуренция както и „най-добрата стойност“ подходи в ценовия задвижва пазара.

• **Демографските промени / работна сила**: трудности при набирането

и задържането на служители / голямото текучество на персонал.

• **Професионализация на сектора:** например професионално обучение и кариерно развитие.

• **Обществените нагласи и правна рамка:** особено по отношение на възможностите за засилване на ролята на частни услуги за сигурност в чувствителни области (напр. критичната инфраструктура и транспорт).

ВЪЗМОЖНОСТИ:

• **Повишено усещане за несигурност:** води до увеличаване на търсенето на сигурност в области, където несигурността расте.

• **По-големи заплахи и рискове за сигурността:**геополитическите нива (местно, национално, международно) и от различни източници (престъпност, тероризма и т.н.)

• **Демографски и социални развития:** въздействие върху изискванията за сигурност: застаряващо население, индивидуализация на обществото, миграционни потоци и т.н. В съчетание с новите проблеми на сигурността от социални промени (например промишлено / икономическо преструктуриране,урбанизацията, новите видове престъпност, и т.н.)

• **Пазарен растеж: намаляване на обществената / капацитета на полицията** (напр. за публичните финанси ограничения) водещо до аутсорсинг и развитие на публично-частните партньорства за осигуряване на сигурността. Специфични сегменти на клиенти (например болници, училища, обществен транспорт и т.н.)

• **Интернационализация/глобализацията** : трансгранично предоставяне и установяване в рамките на единния пазар; желание на клиента за предоставяне на услуги на множество държави.

Аспектите на устойчивостта и околната среда: нарастващото приемане на подхода на жизнения цикъл (например щадящи околната среда продукти, рециклиране, ниско потребление на енергия, ниска консумация на вода и т.н.)

• **Специализация:** повишаване на предоставянето на специализирани услуги за сигурност предоставя възможности за разширяване на пазара (т.е. по-голяма възможност за изнасяне на функции за сигурност)

Проблеми и предложения за решение за развитието на частните услуги за сигурност – Пътна карта

Проблем 1: Липсва приета от бизнеса и регулаторните органи дефиниция кои услуги попадат в обхвата „частни услуги за сигурност“.

Предложение 1: Да се приеме и утвърди от всички заинтересовани участници в процесите дефиниция на икономическите дейност попадащи в обхвата на частните услуги за сигур-

ност.

Предложение за параметри и обхват на сектора:Частната охранителна дейност, мониторинг центрове (с/без реакция с авто-патрули), проектиране и изграждане на системи за сигурност и видеонаблюдение, профилактиката и поддръжката на системи за сигурност и видеонаблюдение, консултанти по сигурността, детективската дейност, услуги по проектиране и изграждане и поддръжка на системи за пожароизвестяване и пожарогасене. Тези услуги да влязат в националния класификатор на икономическите дейности в един раздел – частни услуги за сигурност, като всяка една от тях да бъде в отделен подсектор от този раздел.

Проблем 2: Липсват в класификатора на длъжностите и професиите основни длъжности от частните услуги за сигурност, а са налични други, които не са актуални и/или създават варианти да се извършва дейност в сферата на частните услуги за сигурност, без да отговарят на изискванията.

Предложение 2: Да се направят промени в класификатора. Необходимо е да се преразгледа статутът на длъжности, като: пазач, портиер, пъдар, фейс-контрол, рецепционист и др., които имат сходни функционални задължения с тези на длъжността „Охранител". Въпреки сходните функции обаче, изброените длъжности не попадат под регламентите на ЗЧОД. Този факт подпомага някои фирми да укриват частна охранителна дейност, особено след влизане в сила на задължението звената за самоохрана да се лицензират.

Липсват обаче основни длъжности които са от особено значение за дейността:

- Оператор в мониторинг център;
- Техник по изграждане на системи за сигурност;
- Техник по изграждане на системи за видеонаблюдение;
- Техници по профилактика;
- Охранител в автопатрулен екип;
- Шофьор в автопатрул и инкасов автомобил;
- Ръководител на екип в мониторинг център (началник смяна);
- Консултант по сигурността;
- Пожарна и аварийна безопасност.

Проблем 3: МВР е институцията, която издава лицензи за извършване на частна охранителна дейност и упражнява контрол върху охранителните фирми за спазване разпоредбите в Закона за частната охранителна дейност. Същевременно, съгласно чл. 76 и чл. 77 от Закона за МВР(*към днешна дата чл 92 от ЗМВР и Приложение 1 от ЗМВР*), извършва охранителна дейност като равноправен субект на пазара, с което се превръща в конкурент на юридическите лица, които лицензира и контролира.[2] По новия закон за частна охранителна дейност

от 2018г МВР прави и оценка на съответствието с минимални изисквания за сигурност и безопасност в това число и автомобили и персонал, както и пълен контрол върху дейността : от трудовите договори до договорите с възложителите и начина на функциониране на дружествата.

Предложение 3: Да се отмени правото на МВР да извършва охрана като стопанска дейност (срещу заплащане по договор) и функциите по лицензиране и контрол на ЧОД да се прехвърлят на друга институция, нямаща търговски интереси на охранителния пазар. Да се създаде към министерство на икономиката „Отраслов съвет частни услуги за сигурност“. Сред състава на съвета да са представители на сектора, на МВР, на икономиката и големите работодателски организации. Съвета да направи преглед на наличното и релевантно българско и европейско законодателство и изготви анализ- доклад. Отрасловия съвет на базата на анализа след прегледа на законодателството да стартира процедура по разработване на ново законодателство в сектора, което да прави ясно разграничаване на дейността на търговските дружества като такива, обхвата на лицензионната процедура, без МВР да се намесва в бизнес-процесите,да се разработят процедури съответстващи на законодателството свързани с партньорството на сектора, като естествен партньор на МВР; и в съответствие с актуалното европейско законодателство.

Проблем 4: В сферата на услугите и особено в охранителната дейност най-справедливо и реално за всички участници в процеса /възложител, изпълнител, охранител/ е почасовото планиране, отчитане и заплащане на изпълнената услуга. То е справедливо за работника, защото знаейки колко часа е отработил в месеца /планирани и извънредни/, знае какво възнаграждение ще получи. То е справедливо и за възложителя и изпълнителя, защото почасовото планиране и отчитане е конкретно и прозрачно. Неефективна е практиката и схващането, че възложителят да купува хора, а не услуга. В България са единици фирмите от бранша, за които това е основен начин на планиране и отчитане обема на услугите. Тенденцията е европейската практика да навлезе и при нас, тъй като това е съвременният и перспективен начин за упражняване на този бизнес.

Предложение 4: Въпросът за почасовото планиране, отчитане и заплащане на охранителните услуги е пряко свързан с мотивацията за работа и разграничаване на компетенциите на охранителите. Отчитането на изпълнението на услугите е възможно и в други единици, но е важно тези единици да бъдат унифицирани, за да има сравнимост при избор на изпълнител.

Проблем 5: Начините на подготовка

на персонала[3] /начална и продължаваща/, които се практикуват от фирмите в повечето случаи са формални. Малко са работодателите в сектора, които инвестират в квалификацията на персонала си - изпълнителски, средно ръководен, специалисти, мениджърски. Наличието на специалности в няколко от водещите ВУЗ, специализираните колежи и ЦПО не се използват рационално, а продължават да се предпочитат бивши кадри на държавните структури, с презумпцията за компетентност и в частната охранителна дейност.

Предложение 5: На базата на нормативните промени да се формира образователна програма в липсващото звено между ЦПО и ВУ Да се разширява сътрудничеството между ВУ, колежи и ЦПО и фирмите в сектор «Дейности по охрана и разследване», като се регламентират облекчения или други стимулиращи мерки за работодателите, които инвестират в повишаване квалификацията на служителите си, откриват работни места и дават възможност за кариерно развитие на млади хора в бранша. Въвеждането на валидирането на знанията и оценка на компетенциите също ще съдейства за повишаване на качеството на знанията на служителите. Една такава тенденция ще повлияе положително върху мотивацията на младата и перспективна работна сила за реализация на професионалния потенциал именно в сектор «Частни услуги за сигурност».

Проблем 6: Продължава провеждането на порочни процедури за обществени поръчки и такива в полза на определени участници. В документацията за конкурсите се залагат странни условия, критерии за подбор, технически изисквания и показатели за оценка. Много възложители на ОП за охрана спестяват от сигурност, включително за отговорни и рискови обекти, притискат участниците в обявените процедури за нереално ниски цени на услугите, което в повече от случаите е свързано с човешкия фактор и се отразява негативно върху мотивацията на охранителите за качествено изпълнение на задълженията. Такива възложители, подценявайки потенциалните рискове, не само не получават качествена услуга, но създават предпоставки за нарушаване на нормативни актове от страна на изпълнителите, за увеличаване на «сивия» сектор в охранителния бранш, на нерегламентираната дейност и нелоялната конкуренция.

Предложение 6: Необходими са промени в ЗОП, които да доведат до максимална обективност в процедурите за ОП, да ограничат до минимум порочните практики и конкурсите с предизвестен победител. При подготовка на заданията възложителите да привличат независими експерти, професионалисти по темата на поръч-

ката. А при оценка на документите за конкурса да привличат независими експерти в областта на оценка на рисковете, охранителната дейност, използването на ТСС и мениджмънт на сигурността.

Проблем 7: У нас много охранителни фирми съвместяват охранителната и детективската дейности, но професията „частен детектив“ към днешна дата не е регламентирана в българското законодателство. Няма Закон за детективската дейност, но в никакъв случай не може да се твърди, че дейността, извършвана от частните детективи, е незаконна. Напротив - още от римското частно право е известен принципа „Всичко, което не е забранено, е разрешено“, който намира приложение чрез правилото на чл. 9 от Закона за задълженията и договорите: Страните могат свободно да определят съдържанието на договора, доколкото то не противоречи на повелителните норми на закона и на добрите нрави. И въпреки, че законът не забранява частните детективски услуги, празнотата, която е оставена, влече сериозни негативи, както за лицата предоставящи услугата, така и за клиентите им. Частната детективска дейност е сериозна задача, в която се замесват значителни лични и материални интереси - семейни и бизнес тайни, обстоятелства, уронващи престижа, факти от значение за наказването за извършени престъпления и други. Нормално е да се регулира дейността и лицата, които се занимават с нея, подобно на много други дейности - ЧОД, юристи, медици и т.н.

Предложение 7: Детективските фирми многократно на различни форуми са поставяли въпроса за създаване на Закон за частната детективска дейност, който ще защити правата на клиентите, ще изчисти пазара от така наречените „детективи-ментета“ и ще създаде условия, в които частният детектив може да работи ефективно. В края на 90-те години в НС имаше внесен проектозакон, който обаче остана необсъден. Необходимо е тази услуги да бъдат включени в промените, както в класификатора, като елемент от частните услуги за сигурност, така и в промяната на законодателството.

Проблем 8: Тенденциите в Европа, а вече и у нас са техническите системи за сигурност постоянно да се усъвършенстват, да могат да решават комплексни задачи, контролирани от разстояние, да изместят в някои сектори физическата охрана, като по-скъпа услуга и понякога субективна в действията си. В документите на ЕС за вътрешните услуги, включително и тълкуването “услуги за сигурност“ в нашия закон от февруари 2010 г. (ЗДПУ), монтирането, поддръжката и ремонтът на техническите средства и системи неправилно попада в полето на приложение на Директивата. Трябва реално да се оценява, че на ин-

сталаторите стават известни много подробности от охраняваните обекти - територии, сгради и помещения, охранителни системи, организация на охраната, охраняване активи. Това обстоятелство създава предпоставки чрез нелоялни служители чувствителна информация да достигне и до криминалния контингент.

Предложение 8: Фирмите, които имат основен предмет на дейност монтаж, поддръжка и ремонт на ТСС, извършват тези услуги. Фирмите, за които това не е основна, а съпътстваща дейност, също да лицензират своите служители, заети в нея. Целта е да се елиминира участието на криминално проявени или недостатъчно надеждни лица в дейности, свързани с чувствителна информация. Лицензирането може да се извършва по определени критерии, подобно на заетите в ЧОД, а отговорност за това да носят работодателите/ръководителите на фирмите. В контектста на гореизложеното, препоръчително е и самите фирми, занимаващи се с инсталация, поддръжка и сервиз на охранителни системи, да подлежат на регистрационен режим, с цел повече прозрачност и улеснение при разследване на посегателства[4].

Проблем 9: Организацията на дейностите по пожарна и аварийна безопасност трябва изцяло да се промени и съобрази с тази в европейските страни. Това може да се извърши само ако се създадат проекти и се приемат:

Предложение9: Промени в законодателството свързани с приемането на дейностите по пожарна и аварийна безопасност като елемент от частните услуги за сигурност. Необходимо е да се извършат изменения и допълнения в:

1.Националния класификатор на професиите и длъжностите /НКПД/, като в него се включат пропуснати съществуващи професии, свързани с ПАБ,

2.В списъка на регулираните професии да се добавят всички професии по ПАБ, 3. В КИД да се внесат изменения и допълнения, като се отчетат дейностите по ПАБ.

Предложение 10: За дейностите по ПАБ е възможно и трябва да бъдат въведени стандарти, отнасящи се до квалификацията на човешките ресурси. Същите да послужат като основа при сертификация на персонала, който има право да ги извършва.

Изводи:

Тенденциите за развитие в сектора зависят от икономическите прогнози в България за периода до 2020 г. и, тъй като е прието в дългосрочните бизнес планове да се залагат само положителни прогнози, се счита, че предприятията от сектор „Дейности по охрана и разследване“ ще претърпят и технологично, и организационно развитие, добавящо стойност към произвежданите услуги. Технологиите постепенно ще минимизират чо-

вешкото присъствие в охранителната дейност, а бизнес процесите в предприятията ще бъдат актуализирани и усъвършенствани, вследствие на което ще се разкриват нови работни места в областта на маркетинга, инженеринга, IT, и др.[5]

Липсата на утвърден секторен компетентностен модел, който задължително да се прилага, и използването на лица, заети в сектора на частните услуги за сигурност и в подсекторите като охраната, но извършващи портиерска и пазаческа дейност, девалвират професията и уронват авторитета й на частен вариант на правоохранителна структура.

Мениджърските длъжности в сектора са заети основно от бивши служители на МВР или други държавни органи, които по условие се считат за добри ръководители и са предпочитани за управленски позиции в частните охранителни структури. Охранителната дейност обаче е бизнес като всички останали и изисква от мениджърите не само тясно професионален опит и познания, но и чисто икономически, свързани с управлението на хора и средства с цел постигане на положителен финансов резултат за съответния бизнес процес.

Поддържането на адекватно ниво на сигурност в рамките на всяко общество може да се разглежда като основна (предварителна) предпоставка за създаване на среда, в която граждани и фирми са в състояние и мотивирани да се занимават с икономически дейности, а оттам и за икономически растеж. В този смисъл, сигурността е основно обществено благо, което генерира положителни социални външни фактори и също толкова, посредством разпоредби е свързана с отрицателни външни. На равнището на обществения ред тече дебат относно очакванията по отношение на нивото на сигурност, от това следва да се предвиди и в същото време да се дефинира разпределението на отговорността между частния и публичния сектор при предоставяне на услугите за сигурност.

Зачитайки важната роля на частните услуги за сигурност в днешното общество, може да бъде само в интерес на обществото като цяло, да се намерят адекватни решения за ограничаване на загубите, "навлечени" върху всички търговски страни в тази индустрия до приемливи нива и/или нива които да осигуряват алтернативни финансови източници за покриване на загубите. Очевидно е също, че за да се намери дългосрочно решение на въпросите за критичната отговорност, резултат от терористични атаки или военни действия, е нужна някаква форма на ясна правна рамка в ЕС, респективно и в България за различните сектори.

(Endnotes)

1 Стоян Стойчев, Способности на НАТО и на ЕС за отговор и управление на кризи, монография, ВА „Г. С. Раковски“София, 2015 г., монография, ВА „Г. С. Раковски“.

2 В настоящата публикация не е включен пълен преглед на Закона за частна охранителна дейност приет през 2018 г.,както и поредното изменение на ЗМВР. Данните са базирани на ЗЧОД валиден до 2018г и ЗМВР до 2017 г.

3 Иванов, Г., Подбор, подготовка, оценка и развитие на служители във военната организация, Издателство „ДиоМира“, ISBN 978-954-2977-49-0, 2018.

4 Димов, П., Класификация на информационни продукти и приложен софтуер за проследяване изпълнението на задачите в организацията. Международна конференция - София: ВА „Г.С.Раковски“ 07.04.2017.

5 Димов, П. Приложение на уеб технологии за защита на националната сигурност, ISBN 978-954-2977-47-6, Издателство „Диомира“, 2018.

[6]Geneva Centre for the Democratic Control of Armed Forces (DCAF) Policy Paper – №20 Regulating Private Security in Europe: Status and Prospects;

[7]„Вътрешна стратегия за сигурност на ЕС“ http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:BG:PDF

[8]Стойчев, С., Изследване способностите на НАТО и ЕС за отговор и управление на кризи, Военна академия, 2015, монография, ISBN 978–954–9348–62–0, с. 134.

[9]Програма за действие за укрепване на европейския отрасъл на сигурността http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/863&format=HTML&aged=0&language=BG&guiLanguage=en

[10]Закон за частната охранителна дейност

[11]Закон за министерство на вътрешните работи

[12]БСК Секторен анализ на дейности по „Охрана и разследване“ автор: Татяна Иванова https://iksbg.com/documents-menu/analyses-menu/181-bg-analizes.html

БЪЛГАРСКА Наука

ISSN:1314-1031 Брой 116> ЯНУАРИ 2019

Национален център по мехатроника и чисти технологии

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
НАУКА И ОБРАЗОВАНИЕ ЗА ИНТЕЛИГЕНТЕН РАСТЕЖ