ISSN 1314-3379

КИБЕРОТБРАНАТА КАТО КЛЮЧОВ ЕЛЕМЕНТ ЗА ЗАЩИТАТА НА НАЦИОНАЛНАТА СИГУРНОСТ НА РЕПУБЛИКА БЪЛГАРИЯ

Драгомир Кръстев

CYBER DEFENSE AS A KEY ELEMENT FOR THE PROTECTION OF THE NATIONAL SECURITY OF THE REPUBLIC OF BULGARIA

Dragomir Krastev

Abstract: *At the beginning of the third decade of the XXI st century, cyberspace is increasingly clearly taking shape as a fifth domain for conducting combat operations with a different purpose, intensity, and nature. Countering cyberattacks and hybrid operations directed against the management systems of the Armed Forces of the Republic of Bulgaria requires the application of a complex approach to achieve the necessary managerial, technical-technological, organizational and political capacity to implement a cyber defense policy that is relevant to these of our partner member states of NATO and the EU, as well as building a common one at the Union level.*

Keywords: *cyber security**,** cyber defense, NATO, EU,*

1. Въведение.

Един от основните белези на технологичното развитие на модерните армии е стартиралият от няколко години процес на дигитализация на всички нива. Тук следва да включим новите технологии, които се използват в свързочните и навигационните средства, управлението на операциите и т.н.

От една страна това позволява на щабовете значително да разширят своите способности като максимално оптимизират използването на войските в бойни операции. От друга страна обаче, този процес довежда и до повишена уязвимост на въоръжените сили от кибератаки на противника, които могат да доведат до блокиране на средствата за управление, и свръзка в много по-големи мащаби отколкото в миналите времена на конвенционални военни действия, когато информационните технологии нямат толкова голямо приложение.

2. Изложение.

Трайната тенденция за цифровизацията на системите за водене на бойни действия изкарва на преден план въпроса за значението на киберотбраната като основен елемент във военната сигурност на държавите.

В САЩ доста по-рано от другите страни се поставя въпроса за военните аспекти на киберсигурността. По време на управлението на президента Джордж Буш-младши стартират редица дискусии относно правомощията на въоръжените сили в областта на защита на данните и информационната инфраструктура. Основният проблем е в това, че потенциалният удар може да бъде нанесен върху цивилни обекти от инфраструктурата, а за обезпечаването на киберсигурността там Пентагона не разполага с правомощия.

Така през 2010 г. в структурата на Стратегическото командване на войските на САЩ се създава Киберкомандване, в чийто функции влиза защитата на военната информационно-технологична инфраструктура. През 2017 г. тогавашният президент Доналд Тръмп издига статута на това формирование в ранг на самостоятелно единно бойно командване. Това се налага от факта, че проблемите на киберсигурността излизат от рамките на компетенциите

на Стратегическото командване, свързани преди всичко със сдържането на стратегическите заплахи и се превръща в самостоятелно направление от военната стратегия, като особено внимание се отделя на нападателния киберпотенциал.

Развитие на киберотбраната в НАТО

Развитието на военния киберпотенциал на САЩ оказва забележимо въздействие върху европейските държави-членки на НАТО и ЕС през второто десетилетие на XXI в. През този период в тях се създават военни структури, които отговарят за киберсигурността. Те имат функции по: обезпечаване сигурността на военната информационна инфраструктура, защитата на киберпространството, провеждане на настъпателни кибероперации и т.н.

Редица дейности в сферата на киберсигурността и киберотбраната са предприети и по линия на институционалното сътрудничество в рамките на НАТО. Така през 2012 г. се създава Агенция по комуникациите и информационните технологии (NATO Communication and Information Agency, NCIA), в чийто функции влизат координацията и управлението на ИТ-ресурсите на държавите-членки на НАТО. През последното десетилетие киберсигурността се оформя като една от приоритетните области за Северноатлантическия алианс. През 2014 г. лидерите на държавите-членки за първи път допускат, че кибератаките могат да бъдат основание за прилагането на чл. 5 от Вашингтонския договор. През 2016 г. те приемат, че киберпространството трябва да бъде приравнено на физическото /земно, морско, въздушно и космическо/ пространство. През същата година на срещата на върха на НАТО във Варшава се приема задължението на страните-членки по отношение на киберотбраната (NATO cyber pledge), съгласно което те са длъжни на приемат сходни мерки в областта на развитието на националните киберпотенциали.

Развитие на киберотбраната в ЕС

Киберотбраната представлява третият основополагащ стълб на киберсигурноста съгласно Европейската стратегия за киберсигурност от 2013 г [12]. През 2021 г., Европейския съюз с приемането на документа „Военната визия и стратегия за киберпространството като област на операции“ [2] определя рамковите условия и разкрива целите, способите и средствата, които са необходими за използване на киберпространството като област на операции в контекста на Общата политика за сигурност и отбрана на ЕС (ОПСО). Киберотбраната и използването на свързаните с нея способности на военните операции и киберпространството към днешна дата са прерогатив на държавите-членки на Съюза, като същевременно все повече се разчита на изграждане на по-широка екосистема от технологични способности и промишлен потенциал на ниво ЕС.

Тази екосистема за киберотбрана, която е съставена от военните структури на държавите-членки и се подкрепя от съответните институции, органи и агенции на ЕС (EUIBA), притежава определени специфики в сравнение с други структури /дипломатически, правоприлагащи, неправителствени и т.н./ от гледна точка на киберсигурността и има специфичен модел на управление. Липсата на установена рамка за обмен на информация и формат на сътрудничество между военните екипи на ЕС за реагиране при киберинциденти (milCERT), представлява сериозен проблем с оглед повишеното ниво на киберзаплахи инспирирани от държавни и недържавни субекти.

В тази връзка засиленото междуинституционално сътрудничество в областта на киберотбраната би довело до по-високо ниво на защита за всички потенциално засегнати участници. Затова е от изключителна важност да се предостави възможност за подобен род сътрудничество най-вече чрез осигуряването на подходящи и надеждни средства за обмен

на информация. Организирането на учения и участие в други дейности, които да изграждат атмосфера на взаимно доверие и разбиране.

Друг съществен проблем представлява ограничената взаимна оперативна помощ между държавите-членки. Затова трябва да се помисли за по-нататъшното разширяване на концепцията за създаването на екипи за бързо реагиране в киберпространството в целия Европейски съюз, като се надгради проекта за постоянно структурирано сътрудничество (PESCO). Формиране на екипи за бързо реагиране в киберпространството и взаимопомощ в киберсигурността (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security-CRRT), включително в контекста на чл. 42, § 7 от Договора за Европейския съюз (ДЕС) („клауза за взаимопомощ“) [6], както и в духа на чл. 222 от Договора за функциониране на Европейския съюз (ДФЕС) („клауза за солидарност“) [7].

Опитът от войната между Русия и Украйна, показва, че успешната украинска киберзащита се дължи на ключовата помощ от частния сектор. В тази връзка може да се проучи възможността до каква степен той може да допринесе за повишаване на способностите за реакция на противникови атаки в киберпространството [10].

В този дух са и насоките заложени в Стратегическия компас за сигурност и отбрана [1] приет от Съвета на ЕС през март 2022 г., където се казва, че предвид транснационалния характер на киберзаплахите, ЕС трябва да изгради и развие взаимноизгодни партньорства в областта на киберотбраната, включително изграждане на капацитет за киберотбрана, и да подобри киберустойчивостта на държавите-членки. Това кореспондира и с цифровите приоритети на Европейската комисия, заложени в Стратегията на ЕС за киберсигурност от 2020 г. [5]

Развитие на киберотбраната в Република България

Организацията на командния ред на комуникационните и информационните системи в Българската армия претърпява редица трансформации. Началото е дадено на 24 април 1963 г., когато със заповед на министъра на отбраната е създадена Стационарна опорна комуникационна мрежа /СОКМ/. През 2000 г. е сформирано Командване на стратегическата комуникационна информационна система, което малко по-късно се трансформира в Командване и щаб на Свързочна бригада, която е подчинена на Началника на ГЩ на Българската армия. През 2011 г. се създава Стационарна комуникационна и информационна система, пряко подчинена на министъра на отбраната. На 01 септември 2021 г. е сформирано Командване за комуникационно-информационна поддръжка /КИПКО/, което има следните задачи:

- „Изгражда, менажира, експлоатира и поддържа комуникационно-информационната среда на системата за командване и управление, като предоставя комуникационно-информационни услуги и осигурява комуникационна свързаност и защитен информационен обмен;
- Изгражда и поддържа оперативен център за киберотбрана (MilCERT) за осигуряването на непрекъснат мониторинг, анализ и реакция при инциденти и атаки в киберпространството;
- Формира и участва в екипи за бързо реагиране при киберинциденти в критичната инфраструктура на страната;
- Осигурява привързване на стационарните пунктове за управление към Интегрираната комуникационно-информационна система за управление на страната;

- Осъществява непрекъснат мониторинг, анализ и реакция при инциденти и кибератаки свързани с функционирането на комуникационно-информационните мрежи и системи с контингентите от Българската армия, участващи в операции и мисии извън територията на страната;
- Възстановява ресурсите на стационарните комуникационно-информационни мрежи и системи“ [4].

Въпросите за киберотбраната са разработени в няколко вътрешни юридически акта. В Закона за киберсигурност е дадена легалната дефиниция на понятието „киберотбрана“, а именно: *„комплекс от мерки и способности за защита и активно противодействие на кибератаки и хибридни въздействия върху комуникационните и информационните системи и системите за управление на отбраната и въоръжените сили, както и върху системите за управление на страната при извънредно положение, военно положение или положение на война и върху стратегическите обекти, които са от значение за националната сигурност“* [9]. В чл. 13. (1) от същия закон са разписани правомощията на Министъра на отбраната и Началника на отбраната по отношение на киберотбраната: „Министърът на отбраната провежда държавната политика за защита и активно противодействие на кибератаки и хибридни въздействия върху системите за управление на отбраната и въоръжените сили. Министърът на отбраната организира подготовката за киберотбрана на системите за управление на страната при положение на война, военно положение и извънредно положение.

(2) Министърът на отбраната:

1. организира изграждането и развиването на способности за киберотбрана за защита на системите за управление на отбраната и въоръжените сили, включително на център за киберотбрана и тяхното ресурсно осигуряване;

2. организира координацията и взаимодействието във връзка с изпълнението на поети ангажименти за колективна отбрана на споделеното киберпространство с Организацията на Северноатлантическия договор (НАТО) и Европейския съюз;

3. съвместно с министъра на вътрешните работи и председателите на Държавна агенция „Национална сигурност“ и Държавна агенция „Електронно управление“:

а) изготвя допълнителни изисквания по отношение на планирането и осъществяването на мероприятията по подготовка на киберотбраната и киберустойчивостта на страната при обявяване на извънредно положение, военно положение или положение на война и организира осъществяването на контрола за тяхното изпълнение;

б) организира изграждането, развиването и поддържането на потенциал за защита и активно противодействие, адекватно на съвременните предизвикателства и заплахи в киберпространството.

(3) Министърът на отбраната определя с наредба условията и реда за изграждане и поддържане на киберрезерв с цел повишаване на капацитета и способностите за киберотбрана във взаимодействие с научноизследователската и образователната общност и индустрията. Киберрезервът участва в съвместни обучения и тренировки и може да бъде включван при необходимост за решаване на практически задачи, свързани с киберотбраната.

(4) Началникът на отбраната:

1. организира поддържането на способности за киберотбрана за защита на системите за управление на отбраната и въоръжените сили;

2. възлага интегрирането на задачите по киберотбрана като елемент от стратегическото планиране в плановете за изграждане на отбранителни способности и в плановете за операции на въоръжените сили;

3. организира и координира провеждането на международни или национални занятия, тренировки и учения в областта на киберотбраната“ [9].

В Националната стратегия за киберсигурност „Киберустойчива България 2020” са заложени ангажиментите по отношение на киберотбраната на стратегическо ниво, където: „Президентът, в качеството му на Върховен главнокомандващ на въоръжените сили на Република България получава цялостна информация за състоянието и развитието на националната система за киберсигурност и устойчивост, а при въвеждане на „извънредно положение“, „военно положение“ или „положение на война“ ръководи дейностите по осигуряване на киберустойчивост на държавното и военното управление“ [11].

В точка 3.5.1 „Киберотбрана и въоръжени сили“ от актуализираната стратегия за киберсигурност „Киберустойчива България 2023“ кибератаките и въздействията в киберпространството са определени като „съществен елемент от съвременните хибридни модели за водене на война“ [8]. В същия документ са заложени мерки за обезпечаване и развитие на административен, технически и организационен капацитет и способности за киберотбрана, които да са съвестими с тези на НАТО и ЕС, както и изграждането на общи такива на съюзно ниво. В тях са включени действия по интегриране на киберотбраната в плановете за провеждане на операции от въоръжените сили. „Развитието на център за киберотбрана (milCCIRC) за осигуряване на непрекъснато наблюдение и оценка на сигурността на КИС и формиране на пълна оперативна картина на киберпространството. Развитие на екипи за киберотбрана за своевременна реакция на киберинциденти и атаки и възстановяване на критични комуникационни и информационни услуги. Адаптиране и прилагане на модела на ЕС и НАТО за обединение и споделяне на ресурси на национално ниво, специалисти, технологии, база и развитие на формите на ангажираност – използване на механизма за резерв на въоръжените сили за създаване на специализиран „киберрезерв“ и други форми на ангажиране на киберспециалисти от индустрията, академичните и професионалните среди“ [8].

От изключителна важност за организацията на киберотбраната е тя да е релевантна на непрестанно променящите се заплахи в киберпространството. Според Нас акцентът трябва да бъде поставен върху възможността за реакция на различни по характер елементи на кибервойна като: киберсаботаж, кибершпионаж и киберпропаганда. Геостратегическото разположение на България като външна морска граница на Европейския съюз и нестабилната ситуация в черноморския регион изисква да се обърне сериозно внимание на киберотбраната в морския домейн [3]. Значително внимание трябва да се отдели и на защитата на различните видове обекти от критичната инфраструктура, където тече процес на почти пълна дигитализация на тяхното управление. Тази тенденция допринася за повишаването на рисковете и заплахите за киберсигурността на тези елементи, които са от ключово значение за националната сигурност на Република България. За ефективното справяне с тези заплахи е необходимо да се изгради ефективно сътрудничество с ИТ организации от частния сектор за да може да се използва техният експертен, технологически и технически потенциал.

3. Заключение.

Развитието на информационните и комуникационните технологии, и киберпространството, разглеждано като пети домейн на войната, променят из основи

характера на съвременните военни конфликти. Новите технологии се превръщат в ключов фактор за управлението и оптималното функциониране на въоръжените сили на Република България. В средата на третото десетилетие на XXI в. развитието на основните направления от областта на киберотбраната е заложено почти само в стратегическите документи в сферата на сигурността и отбраната на страната. Необходимо е изготвянето на редица концептуални и приложни документи на базата, на които да се предприемат нужните практически мерки за да може да се изгради съвременна и надеждна система за киберотбрана на Република България.

Използвана литература:

1. A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security, Brussels, 21 March 2022 (OR. en) 7371/22
2. EEAS (2021) 706 REV4
3. GRANCHAROVA, V., LUTZKANOVA, S., Implementing innovative approaches and learning methods in maritime education, Pedagogika-Pedagogy, Volume 95, Number 6s, 2023 ISSN 1314–8540 (Online) ISSN 0861–3982 (Print) p.126- 135. Available from: https://doi.org/10.53656/ped2023-6s.11
4. https://ciscdc.armf.bg/index.php?pg=45 [Accessed 10 November 2024]
5. The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final
6. Treaty on European Union, Consolidated version: Official Journal C 326, 26/10/2012 P. 0001 - 0390
7. Treaty on the Functioning of the European Union, Consolidated version: Official Journal C 326, 26/10/2012 P. 0001 - 0390
8. Актуализирана национална стратегия за киберсигурност „Киберустойчива България 2023”, приета с Решение № 301 на МС от 02.04.2021 г.
9. Закон за киберсигурност, Обн. ДВ. бр.94 от 13 Ноември 2018 г.
10. КАРАДЕНЧЕВА, А., НИКОЛОВ, Ж. Възможности за прилагане на интелигентни системи при комуникационно-информационно осигуряване на Военноморските сили. Известия на Съюза на учените – Варна, серия „Морски науки”, Съюз на учените – Варна, 2021. ISSN 1314-3379, с. 23-25
11. Национална стратегия за киберсигурност „Киберустойчива България 2020”, приета с Решение № 583 на МС от 18.07.2016 г.
12. „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“ (JOIN(2013)1, февруари 2013 г.).

За контакти:
доц. д.н. Драгомир Кирилов Кръстев
Висше военноморско училище “Н. Й. Вапцаров“
гр. Варна, ул. „Васил Друмев” №73
e-mail: drago.krastev@gmail.com