EXAMINING THE EU'S MILITARY CAPABILITIES FOR CYBER DEFENCE

Danko D. Farazov

Joint Operations and Planning Department, National Defence College "G. S. Rakovski", Sofia, Bulgaria, d.farazov@rndc.bg

***Abstract**: The digital environment and enhanced connectivity are undergoing the evolutionary transition from auxiliary functions to basic vital factors for the management and operation of all resources related to human existence. This also necessitates the establishment of protective mechanisms, especially in the military domain, to ensure a sufficiently high level of security protection in the European Union. The study conducted by the European Defense Agency reveals the current state of cyber defense in the military domain and provides the necessary guidelines for development in this area.*

***Keywords**: European Union, European Defence Agency, cyberspace, military cyber defence capabilities.*

ИЗСЛЕДВАНЕ НА ВОЕННИТЕ СПОСОБНОСТИ НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА КИБЕРЗАЩИТА

Данко Динев Фаразов

Въведение

В настоящата публикация ще се разгледа въпроса за киберзащитата в ЕС от гледна точка на военните оперативни способности в съвременните кризи и конфликти от военен характер. ЕС като един от най-големите икономически субекти в света има изградени икономически отношения с всички континенти и няма държава в света, която да не се намира в преки или косвени икономически или социални отношения със страни членки от ЕС. На фона на международния тероризъм, бежанските вълни от Африка, изключително широката и мащабна трудовата миграция към ЕС обусловена от икономически причини, закономерно води до факта, че ЕС се превръща по един или друг начин в участник в редица въоръжени конфликти в горещите точки по света.

Изключителния напредък на комуникационните и компютърни технологии и навлизането им от бита на отделния гражданин до промяна на цялостния облик на обществените отношения, промениха значително и средата в сектора за сигурност. Тези процеси предизвикват промяна и в сферата на сигурността, конкретно това касае всички процеси – от причините за възникване на криза до нейното проявление и управление.

Киберпространството разглеждано от военна гледна точка представлява част от оперативните фактори на средата. Това разбира се има и много по-широко значение не само тясно в рамката на непосредственото значение в оперативната среда, но и в доста по-широко разбиране от гледна точка на IT технологиите, които правят света много по-малък от преди.

Именно това налага *Европейската агенция за отбрана* (EDA) да направи задълбочено изследване и проверка за военните способности на ЕС за киберзащита.

Като допълнително пояснение можем да кажем, че в добавка към техническите уязвимости в системите и софтуера, възникващите и променящи се свойства на самото киберпространство като социално-техническа „мрежа от мрежи" представляват предизвикателство. Уязвимостите

ISSN 2367-7902

възникват и от рисково поведение на хората и организациите. Заплахите могат да дойдат от множество посоки, независимо дали са национални държави, престъпни мрежи или недържавни участници.

Проучването на Европейската агенция по отбрана идентифицира перспективите за сътрудничество в киберзащитата

През месец май 2013 г. *Европейската агенция по отбрана* предостави резултатите от своето проучване на възможностите за военна киберзащита. Използвайки задълбочена методология, проучването определя степента на „готовност за киберзащита“ на двадесет участващи държави-членки и различни организации на ниво ЕС. Направеното проучване показва противоречиви резултати по отношение на военните способности за киберзащита на национално и европейско ниво. В следствие на това проучване се препоръчва засилване на сътрудничеството, обмена на информация и предлага начини за прагматично обединяване и споделяне на някои ключови възможности за киберзащита. Изследването подкрепя значимостта на дейностите по киберзащита, започнати от *Европейската агенция по отбрана* в областите за адекватно обучение на кадри и ситуационна осведоменост при кибер атаки. Авторите определят важността кибер защитата по следния начин: „Киберпространството може да бъде описано като пето измерение на войната, еднакво критично за военните операции като сушата, морето, въздуха и космоса. Нашето проучване разкрива важни пропуски във военните способности за киберзащита в целия ЕС. Агенцията предлага на държавите-членки редица проекти за сътрудничество в областта на възможностите за киберзащита, както и в областта на научните изследвания и технологиите“, казва Петер Раунд от *Европейската агенция по отбрана*. Едногодишното проучване има за цел да установи нивото на разбиране и възможностите за киберзащита в рамките на ЕС, за да се подпомогне напредъкът към постигане на по-високо ниво на способности в целия ЕС.

Методологията на изследването включва проучвания на различните организации на равнище ЕС, участващи в дейностите по киберзащита в контекста на мисията по *Общата политика за сигурност и отбрана*, както и събиране на данни за възможностите за киберзащита от страните-членки. Изследването се извършва чрез преглед на документи, интервюта и въпросници. Информацията за киберзащитата е анализирана в съответствие с общоприетата военна рамка на способностите, известна като *Отбранителни линии на развитие*.

Резултати:

- Предстои създаването на основополагащи и дълготрайни водещи принципи на базата, на които да се изгражда киберзащитата;
- Важен момент е обучението на персонал, който да е тясно насочен в тази дейност;
- Изграждането на стандарти и процедури за оперативна съвместимост е задължително условие за създаването на дори и на минимални способности;
- В областите на доктрините е от изключителна важност създаването на изпълними и отразяващи реалната среда, и проблематика нормативни документи;
- Организационните структури предстои да бъдат изградени по начин, който съответства на регламентиращата нормативна база, това изисква и по-дългосрочни усилия за създаването им;
- Необходимо е при обучението да се създаде и обособи дългосрочни развитие и изграждане на съответното кариерно поле;
- В изграждането на инфраструктурата на мрежовата среда към момента също липсва налагането и стриктното спазване на стандарти за киберсигурност;
- Профилите на отделните държави са класифицирани и не могат да бъдат предоставени;
- В Европейски съюз и страните-членки съществува към момента сложна система от организационни структури, които не работят в синхрон и още повече тези структури нямат ясно дефинирани цели, задачи и мисии. Това се дължи основно на факта, че липсва ясно обособена доктринална и нормативна основа;

ISSN 2367-7902

- В страните-членки използването за киберсигурност на специфични военни стандарти и инструменти все още е слабо разбрано.

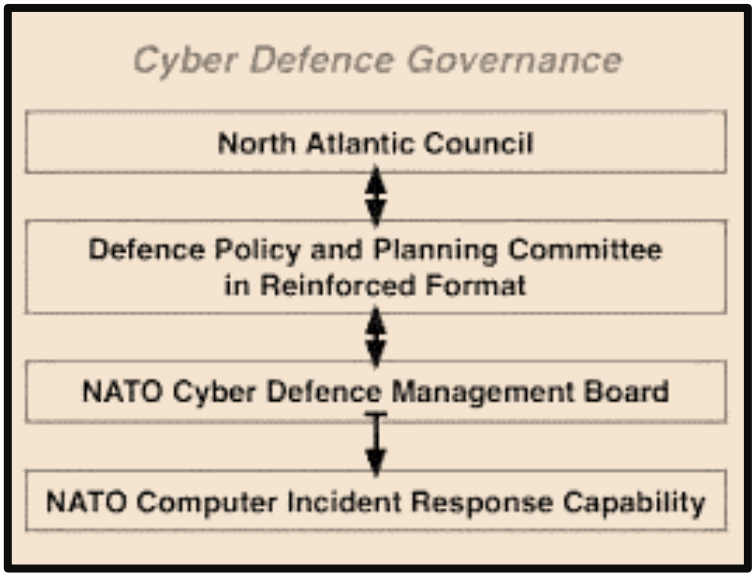
Като бъдещи препоръки може да се каже че военната киберзащита на европейско ниво е в относително ранен стадий на развитие. Следователно проучването прави общи препоръки, които се отнасят главно за разбирането на проблематиката, те включват подобряване на защитата на мрежовата среда, развитие на способностите за разузнаване, развиване на способностите за реагиране при инциденти, създаване на култура на киберсигурност, приемане на стандарти и процедури за засилване на връзките между НАТО и ЕС по въпросите на киберзащитата. На национално равнище трябва да се обърне по-голямо внимание на процеса на обучение и образователни инициативи в тази посока. Страните-членки се насърчава да задълбочат обмена на информация, решения за техническа съвместимост, както и обединяването и споделянето на способности, това включва и споделянето на процедури в мисии, ръководени от ЕС.

В рамките на разглежданата тематика, особено внимание трябва да се обърне и на мобилните устройства, които вече представляват едни портативни компютри и все повече изпълняват функциите на традиционните компютри. По този начин те създават допълнителни заплахи за киберсигурността. Поради техните спецификации те са изключително уязвими и надеждността им се гарантира много трудно. [1]

Европейската агенция за отбрана (EDA) заедно с *RAND Europe* и *Fondation pour la Recherche Stratégique* провеждат обстоен и задълбочен анализ на способностите, включително и концепциите в областта на киберзащитата в страните-членки от ЕС. Участие вземат широк спектър от експерти, които са специалисти в различни области, като по-голямата част са извън военната област. Това се налага поради комплексния характер от заплахи и обособилата се вече значително размита граница между военните и невоенните измерения на киберзаплахите. Разработено е за целите на проучването методика за верификация, която позволява да се определи възможно най-обективно киберзащита под формата на „модел за адекватност“. За определяне на „способностите“ е използвана стандартизирана военна рамка. На тази основа са определени и следните няколко важни констатации:

- Има тясна връзка между осведомеността на всяка отделна страна-членка относно нейната киберзащита и броя на показателите за способности, които тя може да покрие.
- Много страни от ЕС са създали организационни структури, които да се занимават с киберзащита. По-голямата част от страните-членки имат в своите министерства на отбраната отдел, отговорен за задачите свързани с киберзащитата, като това е свързано с натрупания опит на националните екипи за компютърно реагиране при извънредни ситуации (CERT).
- Изостава нормативната база (само 6 от 20 държави имат конкретна стратегия за киберзащита, а 5 от 20 имат доктрина за киберзащита).
- Необходимо е отделяне на особено внимание на обучението на кадрите (9 от 20 държави имат специалност киберсигурност като кариерно поле на развитие), както и изградена оперативната съвместимост (само 5 от 20 участваха в учения в целия ЕС).
- *RAND-Europe* се ангажира в редица последващи проекти, за да предостави съвети на *Европейската агенция за отбрана*, как различните държави могат да повишат способностите си за киберзащита. [2]
- Осигуряване на оперативна съвместимост със структурите на НАТО за киберсигурност като част на ЕС от структурите на Алианса [3], представени на фигура 1.

ISSN 2367-7902



Фигура 1 : Структурна организация за киберсигурност на НАТО

Въведение в киберзащитата

Киберпространството днес често се описва като петото измерение на воденето на бойни действия, еднакво критично за военните операции както сушата, морето, въздуха и космоса. Успехът на военните операции във физическите области е все повече в зависимост от наличието и достъпа до киберпространството. Въоръжените сили разчитат на киберпространството както като потребител, така и като домейн за постигане на мисиите за отбрана и сигурност. Следователно Стратегията за киберсигурност за Европейския съюз, която е публикувана през февруари 2013 г., подчертава: „Усилията в областта на киберсигурността в ЕС също включват измерението за киберзащита.“ Киберзащитата е един от десетте приоритета в *Плана за развитие на способности* (CDP) на *Европейската агенция за отбрана* (EDA). Проектният екип на *Европейската агенция за отбрана* и представителите на участващите държави-членки са отговорни за съвместното разработване на тези възможности за киберзащита в рамките на *Общата политика за сигурност и отбрана на ЕС* (CSDP). Съвкупността от експерти и технологии за изследвания на възможностите в областта на киберзащитата осигуряват цялата дейност чрез съгласувани процедури и механизми. Всичко това е позиционирано до съществуващите и планирани усилия на участващите държави, институциите на ЕС и НАТО. Като се има предвид, че заплахите са многостранни, се предприема цялостен подход, който се стреми да засили взаимодействията между гражданския и военния домейн при защитата на критични способности.

Цел и методология на *Европейската агенция по отбрана*

Европейската агенция за отбрана възлага едногодишно проучване за установяване на задълбочено разбиране на възможностите за киберзащита от отделните държавите. Целта е да се подпомагане напредъка към постигане на по-високо ниво на способност за киберзащита в целия ЕС. В проучването участват двадесет държави. Това включва проучвания на различните организации на равнище ЕС, участващи в дейности по киберзащита в контекста на мисиите за *Общата политика за сигурност и отбрана на ЕС*, както и събиране на данни относно възможностите за киберзащита във всяка държава-членка. Изследването се извърши чрез преглед на документи, структурирани интервюта и разработване на въпросници, разпространени до държавите-членки на ЕС, участващи в екипа на проекта за киберзащита на *Европейската агенция за отбрана*. Информацията за способността за киберзащита е анализирана в съответствие с общоприетата военна рамка от функционалности допринасящи за способността за отбрана, известна като *Отбранителни линии на развитие* (DloDs). Това включва следното: доктрини, структурна организация, обучение, материална база, водещи специалисти, оперативна съвместимост (DOTMLPF). За определяне на степента на „Кибер-готовност“, проучването използва модел за определяне на развитието на способностите от пет стъпки с шестдесет и девет теглови показатели, които определят степен-

ISSN 2367-7902

та на изградените способности, това се осъществява в рамката на военния модел DOTMLPF-I или известен още като *Системата за интегриране на съвместните възможности* (JCIDS Process), за да се постигне необходимия обхват от съвкупни дейности. Всяка държава е качествено оценена спрямо този модел с теглови показатели. Докладът от проучването, включително некласифицирано обобщение, е представен през май 2013 г. Профилите за всяка участваща държава-членка са предоставени в класифициран доклад.

Изследването открива сложна и разнообразна картина по отношение на способността за киберзащита както на ниво ЕС, така и в рамките на отделните държави.

Що се отнася до киберзащитата в рамките на организациите на ЕС, проучването подчертава сложната оперативна настройка между *Европейската агенция за отбрана*, *Европейската служба за външна дейност* (EEAS), *Генералния секретариат* на *Съвета на ЕС*, *Европейската комисия* и свързаните с нея агенции на ЕС като *Европейската Агенция за мрежова и информационна сигурност* (ENISA), *Европейски център за киберпрестъпност* (EC3) и *Екипът за реагиране на компютърни аварийни ситуации* (CERT-EU). Докато анализът на заплахите и възможностите за събиране на кибер-разузнаване се развиват и разширяват, така се осигурява и по-задълбочено и адекватно реагиране на инциденти в киберпространството. Разкрива се също, че културата на добрите практики за киберсигурност трябва да се поддържа, и използването на специфични военни стандарти и инструменти все още е слабо разбрано и усвоено.

Констатирано е, че участващите държави в проучването имат противоречиви и разнопосочни схващания по отношение на военните способности за киберзащита. Най-общо казано, там където институционалните органи и лицата, на които е делегирано правото да вземат решения, са запознати с проблематиката на киберсигурността, възможностите за киберзащита на тези държави са по-добре развити и напреднали. Двадесетте държави имат силни страни в областите на лидерството, специалистите и оперативната съвместимост. В останалите области, като доктрините, организацията и обучението има определени слабости и изоставане, което може да бъде свързано с факта, че тези три области изискват по-сложни и по-дългосрочни усилия за създаване на организационни структури. На последно място в сферата на изграждането на инфраструктурата, която и до днес остава с много слабости по отношение на защитата си и е необходимо адекватно и цялостно, архитектурно решение за развитие и бъдещо изграждане.

Военната киберзащита в ЕС е в сравнително ранен стадий на развитие. Следователно издадените препоръките са в ориентировъчни аспекти и засягат високите нива, които се считат за поважни в процеса за развитие на киберзащита на ниво ЕС, и те са подробно описани в класифицирания доклад. Общите препоръки са следните:

- Подобряване на защитата на мрежите в ЕС, чрез централизирано управление на мрежи за обмен на данни;
- Укрепване на способността за разузнаване, чрез разработване на модел за сътрудничество с *Европейския център за киберпрестъпност* и *Европейската агенция за мрежова и информационна сигурност*;
- Задълбочаване на способностите за реагиране при инциденти, чрез механизми за ранно откриване и предупреждение;
- Създаване на специфична култура за киберсигурност. Това се постига чрез изграждане на взаимодействие между свързани структури;
- Приемане на стандартите и инструменти за сигурност на ISO2700x и бъдещо развитие на тези стандарти заедно с НАТО;
- Укрепване на връзките между НАТО и ЕС по въпросите на киберзащитата, като се провеждат съвместни учения, и съвместно управление на кибер кризи.

Препоръки към страните в ЕС:

- Държавите се насърчават да разработват свои доктрини за киберзащита в тясно сътрудничество с останалите страни-членки;

ISSN 2367-7902

- Трябва да се извършва преглед на това как се развиват организационните структури, за да се осигури координиран отговор във всяка държава, инициативи за обучение и образование, както на оперативно, така и на висши командни нива;
- Държавите-членки могат да обмислят обмен на информация за решения свързани с обединяване и споделяне на способности за киберзащита, особено в ръководените от ЕС мисии;
- Обмен на информация за практиката за набиране и развитие на специалистите в областта на отбраната чрез създаване на „Кибер резерви“;
- Процесите и споделените процедури при ескалация на средата могат да бъдат обменяни и развивани, за да се постигне единно разбиране в цялостния контекст на киберзащитата, особено на ръководените от ЕС операции;
- Трябва да се обърне по-голямо внимание на аспектите на оперативната съвместимост, в частност на невоенните организации.

Следващи стъпки

Направените констатации се анализират и оценяват от държавите участващи в това изследване и от *Европейската агенция за отбрана.* Очаква се много поуки да бъдат извлечени от препоръките на проучването, особено в области, където държавите могат да се възползват и от тясното сътрудничество с *RAND-Europe*. Някои действия вече са предприети, особено в областта на обучението и ученията, главно насочени към изграждане на европейска култура за киберзащита.

Проекти за киберзащита на Европейската агенция по отбрана (Cyber Defence Projects)

Агенцията работи в областта на възможностите за киберзащита и в областта на научните изследвания и технологиите (R&T).

Обучение - *Европейската агенция за отбрана* провежда структуриран анализ на потребностите от обучение по киберзащита (TNA), за да се изгради надеждна учебна програма за обучение по киберзащита. Това трябва да надгражда съществуващия капацитет за обучение в институциите на ЕС и да се осъществява в тясно сътрудничество с *Кооперативния център за киберзащита* (Cooperative Cyber Defence Center of Excellence) в Талин. Идентифициран е и първият съвместен проект, който има за цел да увеличи наличието на виртуални обучения за киберзащита в по-широк обхват (Cyber Ranges) за обучение на специалисти по киберзащита за нуждите на отделните държави.

Ситуационна осведоменост - *Европейската агенция по отбрана* понастоящем работи и върху ситуационната осведоменост в кибер операциите по проекта за *Общата политика за сигурност и отбрана на ЕС* и как да интегрира киберзащитата в процеса на военно оперативно планиране. И по двата аспекта *Европейската агенция за отбрана* съвместно със държавите участващи в изследването активно допринасят за фокусиране в областта на киберзащитата за развитие на многонационалните способности, ръководена от САЩ (MCDC). Целта е повишаване на ситуационната осведоменост при кибер атаки (Cyber SA kit) за да интегрира тези функции и да предостави обща и стандартизирана платформа за планиране и управление на киберзащитата, която позволява на ръководните кадри и техния персонал да използват в операции за изпълнение на задачите, свързани с киберзащитата, през всички етапи на управление на дадена криза.

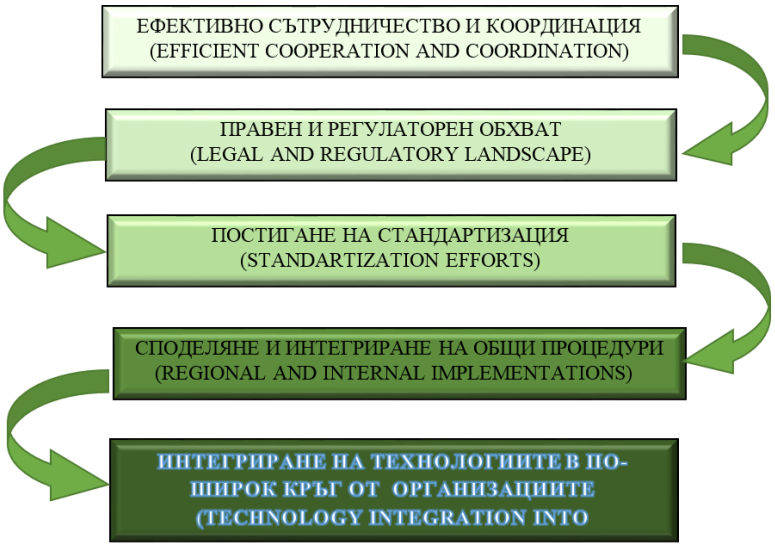
Програмата за изследване на киберзащитата (CDRA) - Технологиите за киберсигурност са очевидно свързани както с гражданската, така и от военната област („двойна употреба“). Тъй като гражданските изследвания вече са представени и планирани в изискванията на *Рамковата програма за научни изследвания на ЕС*, тъй като при наложените ограничения на финансовите ресурси, ще бъде изключително важно да се насочат точно усилията за научноизследователска и развойна дейност към конкретни способности. Програмата за изследване на киберзащитата ще разгледа тези аспекти и ще предложи пътна карта за следващите 10 години.

Правителствата и техните институционални органи за откриване на постоянни заплахи (APT) имат основна задача намирането на злонамерен софтуер, насочени най-вече към кибер шпионаж. Основният проблем тук се заключава, че заплахите или са открити твърде късно, или изобщо не са открити. Ранното откриване е от решаващо значение за концепцията за правилно

ISSN 2367-7902

управление на риска. Следователно Агенцията подготвя обсъждането на предложения за анализ и идеи за възможни решения.

Днес много задачи за откриване на кибер атаки се изпълняват в рамките на отделни организации и има изключително малко междуорганизирано споделяне на информация. Въпреки това, обменът на информация е една от решаващите стъпка към постигане на задълбочено разбиране на мащабните кибератаки и поради това се разглежда като една от ключовите концепции за защита на в бъдеще на мрежите показано на фигура 2. Откриването на скрити кибератаки и нов зловреден софтуер, генериране на ранни предупреждения, съвети за това как да се защитят мрежите и избирателно изпращане на данни и информация за заплахите са само част от механизмите, които трябва да се интегрират в единна система.



***Фигура 2**. Пет степенен модел за изграждане на киберзащита*

Технически форум за технологии в киберзащитата представлява научноизследователска и развойна дейност свързана с комуникационните и информационните технологии (ICT) дава на държавите платформа за обсъждане и подготовка на съвместни технически проекти в областта на киберзащитата. Докато редица такива предложения се очакват от пътната карта на *Програмата за изследване на киберзащита*, изискването за сътрудничество в моделирането и симулацията на киберзащита (M&S – modelling and simulation) вече е напълно възможно.

Дейности на Европейската агенция по отбрана.

На основата на направения качествен анализ на наличните реални способности, както и идентифицираните слабости и пропуски се насочва изграждането на ясно разбиране и полагането на основите за киберзащитата като един от основните приоритети на *Агенцията*. В допълнение към дейностите, извлечени от *Плана за развитие на способности* на *Европейската агенция по отбрана*, като изследванията върху човешките фактори в киберзащитата, изготвянето на програма за изследвания в областта на киберзащитата и общата учебна програма за обучение, се акцентира върху най-належащите пропуски, установени в проучването. Следователно *Европейската агенция по отбрана* започва три ad-hoc проекта с държавите-членки:

(1) **Проектът за *кибер обхват*** цели обединяване и споделяне на настоящи и бъдещи ресурси за обучение по киберзащита, упражнения и тестове с цел повишаване на достъпността и ефективността на съществуващите способности, както и интегриране и подобряване на общото ниво на обучение за киберзащита в ЕС.

(2) **Инициативата за *ситуационна осведоменост* в кибер пространството**, която има за цел да предостави, обединение и споделяне в обща и стандартизирана платформа за планиране и управление на киберзащитата. Тя позволява на командирите и щабовете в ръководените от ЕС

ISSN 2367-7902

операции да изпълняват функционалните си задължения, свързани с киберзащитата, през всички етапи на ръководената от ЕС военна операция.

(3) **Инициативата за проект** „***Разширено и надеждно откриване на заплахи*** (APT-D - Advanced Persistent Threats Detection)“ се фокусира върху подобрените възможности за ранното им откриване.

Под председателство на Европейския съюз през 2013 г. *Европейската агенция по отбрана* бе домакин на конференция на високо равнище за сътрудничество в областта на киберсигурността в Европейския съюз.

Трябва да се отчете и факта, че през последните години се появи и терминът „кибервойна”,които навлезе масово в употреба не само сред военната, но и сред цивилната общност – експерти по информационна сигурност, политици, средства за масова информация. Освен това кибервойните станаха една от най-обсъжданите теми в социалните мрежи и интернет като цяло. Но в тълкуването съществуват сериозни разлики. Сред политиците, медиите и обикновения потребител е разпространено „широкото” разбиране – всяко противоборство в киберпространството. Специалисти и експерти отнасят към кибервойната някои многоаспектни и сложни информационни компании, насочени към изменение на ценностната ориентация, политическите предпочитания, а даже и културата. И не на последно място – към кибервойните причисляват и битките за репутация, наречени още „войни на брандовете”, които се водят между различни бизнес групи и корпорации. [4]

Като положителен пример може да се даде откриването в Бундесвера на 05.04.2017 г. Киберкомандване (фиг. 3), което ще достигне пълния си капацитет от възможности до 2021. [5]

Фигура 3 . Киберкомандване на Бундесвера.

В заключение трябва да се каже, че с навлизането на все повече и повече на компютърните технологии и цифрови комуникации, проблемите със сигурността ще заемат по-централно и основно място за качеството на работата. Поставеното начало през 2013 г. за изграждане на единна система и стандарти по киберсигурност и защита на мрежите е изключително важно, тъй като показва ясно сериозността на проблема, който тепърва ще започне да се сблъскваме в областта на отбранителната.

СЪКРАЩЕНИЯ:

1. ЕС – Европейски съюз
2. EDA- European Defence Agency
3. CDP- capability development plan
4. CSDP-common security and defence policy
5. DloDs - Defence Lines of Development
6. DOTMLPF- Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities.
7. JCIDS Process – The Joint Capabilities Integration Development System
8. EEAS – European External Action Service
9. ENISA – European Network and Information Security Agency

ISSN 2367-7902

10. EC3 – European Cybercrime Centre
11. CERT-EU - Computer Emergency Response Team
12. R&T- research & technology domain
13. TNA-Training Need Analysis
14. MCDC – Multinational Capability Development Campaign
15. Cyber SA kit – Cyber Situational Awareness kit
16. CDRA- Cyber Defence Research Agenda
17. APT- Advanced Persistent Threats
18. ICT- communication and information technology

References

1. Ivanov, Galin, (2015), Cybersecurity of mobile devices. "KSI Jurnal of Knowledge Society", Veliko Tarnovo, ISSN 2367-7198
2. https://www.rand.org/randeurope/research/projects/eu-military-cyber-defence.html, посетено на 20.05.2020 г
3. https://securityaffairs.co/wordpress/20705/cyber-warfare-2/nato-attack-response-teams.html, посетено на 20.05.2020 г.
4. Козарева-Арменчева Илина., 2015, Киберсигурността – ключовият въпрос в глобалното общество, София: ВА „Г. С. Раковски", ISBN 978-954-9348-67-5
5. https://www.dw.com/en/bundeswehr-cybersecurity-center-trains-elite-counterhackers/a-43210036, посетено на 20.05.2020 г.

ISSN 2367-7902