DOI: 10.58894/kba5x937

ISSN 2535-0587
МЕДИИ И ЕЗИК
ЕЛЕКТРОННО СПИСАНИЕ ЗА НАУЧНИ ИЗСЛЕДВАНИЯ ПО МЕДИЕН ЕЗИК

Брой 19
Информационната сигурност
2026

Статията на тема: „Влиянието на информацията и дезинформацията върху комуникационните процеси на международната среда за сигурност“ се публикува с подкрепата на Фонд „Научни изследвания“ при МОН по проект (Договор № КП-06-НП7/29 от 08.12.2025 г.), одобрен в конкурсната сесия „Българска научна периодика – 2026“ за издаване на рецензираното научно сп. „Медии и език“ (ISSN 2535-0587). Фонд „Научни изследвания“ не носи отговорност за съдържанието на материалите.

Влиянието на информацията и дезинформацията върху комуникационните процеси на международната среда за сигурност

Росица Филатова
Софийски университет „Св. Климент Охридски“
rositsafilatova@gmail.com

КЛЮЧОВИ ДУМИ

информация
дезинформация
международна сигурност
комуникация
киберсигурност

РЕЗЮМЕ

Докладът разглежда различни аспекти на влиянието на информацията и дезинформацията върху комуникационните процеси на международната следа за сигурност. Специално внимание е обърнато върху дефинирането на понятието сигурност и се разглеждат различни проявления на информацията и дезинформацията. Посочва са ролята на киберсигурността в борбата с хибридните заплахи. Основната задача на международните актьори е да се противопоставят на разпространението на невярна информация и да създадат такива способи, които да защитят международната сигурност.

Увод

Цел на настоящото изследване е с исторически и настоящи източници да разкрие и обоснове различните аспекти и проявления на комуникационните процеси в международната среда за сигурност. Поставя се акцент върху влиянието на

дезинформацията и хибридните войни върху информационната сигурност и вредите, които те причиняват за поддържането на международния мир и сигурност.

Тази цел ще бъде постигната с разглеждането на поставените изследователски задачи, които включват дефиниране на понятието „сигурност“, отделяне на специално място на киберсигурността и киберпространството, които са засегнати от влиянието на дезинформацията и хибридните войни, както и ролята на основните международни актьори.

Основните методи използвани в настоящото изследване са теоретичният и историческият. С помощта на тези методи са направени заключения и са посочени актуални дефиниции, които са залегнали в основата на изследването. Регистрирани са индивидуални организационни заслуги и е обоснована необходимостта от интериснтитуционално сътрудничество. Разкрива се, доколко различните аспекти на комуникационните процеси и системи оказват влияние върху поддържането на международния мир и сигурност.

Сигурност и информационна сигурност

Бари Бузан и Оле Уевер дефинират сигурността като дейност, действие, или движеща сила, която извежда политиката извън установените правила на играта и очертава новите проблеми като нов тип политика. Авторите въвеждат понятието „секюритизация“ и го дефинират като екстремна версия на политизацията и като успешен речеви акт, посредством който, в рамките на една политическа общност, се изгражда разбирателство между субектите по повод нещо да бъде третирано като екзистенциална заплаха за даден значим обект и да даде право за призоваване към неотложни и извънредни мерки за справяне със заплахата. (Слатински, 2011, с. 89-118) Понятието „секюритизация“ въвежда Оле Уевер през 1995 г. То е ключово в Копенхагенската конструктивистка школа в сигурността и международните отношения. (Пак там)

Според Бузан и Уевер обществените проблеми биват: (а) не-политически; (б) политически, и следователно изискват управленско решение и ресурси, а в някои случаи и друга форма на общностно, комунално управление; (в) секюритизирани, т.е., превърнали са се в екзистенциална заплаха, изискваща извънредни мерки и действия, с проекции извън регулярната политическа процедура. (Пак там)

Всеизвестен факт е, че до днес липсва общоприета дефиниция за понятието „информация“. А то е методологичен инструмент не само за комуникационната наука, а и за всички науки за човека. И ако методът по дефиниция е знание за общото, прилагано при изучаване на частното или конкретното, се оказва, че частните въпроси за човека, сред които познанието и комуникациите, не могат да се

изучават с обективно изработен и общовалиден метод. Съответно, резултатите от изследванията по конкретните въпроси на познанието и комуникациите трудно биха се наложили като обективен научен аргумент. (Цветкова, 2011)

Може да се каже, че информацията (от латински: *informatio* – разяснение, изложение, осведоменост) е понятие, свързано с обективното свойство на материалните обекти и явления (процеси) да пораждат многообразие от състояния, които могат да се предават на други обекти чрез взаимодействия и да се запечатват в тяхната структура. (Уикипедия)

При информационната сигурност, компютърните системи и мрежи са едни от най-високо технологичните продукти на човечеството. Освен всички предимства, които предлагат, те имат и редица недостатъци. Проблемите със сигурността под формата на зловредни програми, загуба на правото на неприкосновеност на личния живот, изпращане на нежелана реклама или спам, засягат почти всеки компютърен потребител. (Войноховска, Цанков, 2014, с. 71)

Сигурността е свойство на една система да противостои на външни или вътрешни дестабилизиращи фактори, които могат да доведат до нейното нежелателно състояние или поведение. Това важи и за сигурността на информационните системи. (Пак там)

Една успешна организация трябва да има следните няколко слоя на сигурност за защита на своята дейност:

- Физическа сигурност – защита на физическите обекти или области от неоторизиран достъп и злоупотреби.
- Сигурност на персонала – защита на хора или група от хора, които имат оторизиран достъп до организацията и нейните операции.
- Сигурност на операциите – защита на определена операция или серия от дейности.
- Сигурност на комуникациите – защита на средата за комуникация, технология и съдържание.
- Мрежова сигурност – защита на мрежовите компоненти, връзки и съдържание.
- Информационна сигурност – защита на конфиденциалността, интегритета и достъпността на информацията при съхранение, обработване или пренасяне. Това се постига с прилагане на политики за сигурност, обучение и повишаване на знанията и чрез помощта на технологиите. (Пак там)

Киберсигурност – развитие и приложимост

Киберсигурността се отнася до дейностите, необходими за защита на мрежите и информационните системи, потребителите на такива системи и други лица, засегнати от киберзаплахи. (European Union, EUR-Lex) Киберпространството се счита за петата област на военни действия и е съпоставимо по важност за военните операции със сушата, морето, въздуха и космоса. Това е област, обхващаща всичко от информационните и телекомуникационните мрежи и инфраструктури заедно с поддържаните от тях данни до компютърните системи, процесори и контролери. Киберпространството се превърна и в силно оспорвана стратегическа област и сфера на стратегическа конкуренция. Освен това цифровата и физическата инфраструктура са взаимнозависими, което означава, че значителни киберинциденти могат да предизвикат смущения или вреди на критична инфраструктура. (Европейски съвет)

Мениджмънтът на киберсигурността представлява система от взаимнообвързани процеси по управление на информационни ресурси за постигане на широкообхватна цел по контрол на достъпа, осигуряване цялостност и наличност на тези ресурси. Поради широкообхватната цел на мениджмънта (решаването на задача с голяма сложност) се прилагат методи на управление, обединяващи процесите по планиране на ресурси и

прилагане на технологии. (Калчев, Цветков, 2022, с. 12-14) Елементи на мениджмънта на киберсигурността[i]:

- наличните информационни активи на организацията;
- политиката по киберсигурност на организацията;
- средствата, с които се реализира политиката по киберсигурност на организацията (организационни, технически и др.);
- планиране на ресурсите по киберсигурност на организацията;

Факторите, определящи осъществяването на киберзащитата, са три: човешки, технологични и законодателни. Човешкият фактор има съществена роля за осигуряване киберсигурността на информационно-комуникационните системи. Той е зависим както от морално-етичните характеристики на отделния човек, така и от нивото на неговата подготовка. Човешкият фактор е пряко свързан с процеса на създаване на организация за опазване на чувствителна и конфиденциална информация. Достъпът до обработваните и съхраняваните данни и информация трябва да е съобразен с изискванията на Закона за защита на класифицираната информация, а именно да се спазва принципът „необходимост да се знае“. (Пак там)

Необходимо е да се предвидят и изпълняват мерки за архивиране и съхраняване на данните с цел тяхното бързо и надеждно възстановяване в случаи на кибератаки или след възникнали сривове, а също така следва да се алгоритмизират и документират процедурите за възстановяване. Техническите и технологичните средства са свързани основно с хардуерната и софтуерната защита на информационните и комуникационните системи и могат да се обобщят по следния начин: средства за физическо осигуряване на компютърните системи срещу кражба, несанкциониран достъп и некоректно използване. (Пак там)

Средства за контрол на достъпа – защитни стени, пароли, използване на биометрични данни. Необходимо е да се съгласува съществуващото национално законодателство с това на водещи страни в света в частта си за наказателните мерки спрямо специалистите, които създават и разпространяват злонамерен софтуер с цел нанасяне на щети и опит за неправомерен достъп до данни и информация, а също така да се актуализира в съответствие с динамичната промяна на условията за сигурност. (Пак там)

Информационната система (ИС) представлява съвкупност от софтуер, хардуер, данни, персонал, процедури и мрежи, които правят възможно използването на информационните ресурси в организацията. Тези шест критични компонента позволяват информацията да бъде въвеждана, обработвана, извеждана и съхранявана. Всеки от тях има своите предимства и недостатъци, характеристики и приложения. (Войноховска, Цанков, 2014, с. 73)

Киберпространството е една реалност, в която националните интереси – военни, дипломатически, икономически и социални са уязвими от атаки и са подложени на рискове. Като интеграционни структури, чийто страни членки са измежду най-високо развитите в използването на кибер пространството, ЕС и НАТО са и едни от най-уязвимите от кибер атаки. В тази връзка те следва да предприемат активни стъпки за приоритетна подготовка на своите Въоръжени сили за действие в сложна кибер среда. Планирането, подготовката, обучението и тренировките могат да бъдат резултат само от добра политика и сътрудничество. Прогресът в тези области следва да е постоянен и с висока скорост, за да следва промените в кибер средата. Изискване на Концепцията на НАТО за кибер отбрана е т.нар. „Отбрана в дълбочина“. Такава стратегия следва да покрие всички нива на кибер пространството, от международните организации като НАТО, ЕС, ООН, до държавите и частния сектор. НАТО и ЕС следва да ускорят усилията си, да отговорят на опасностите от кибер атаки чрез защита на своите комуникационни системи и системи за командване и управление, да помогнат на страните членки да подобрят националните си способности за предотвратяване и възстановяване от кибер атаки, и създавайки поредица от кибер способности да са в състояние да разкриват и предотвратяват такива атаки. (Панайотова, 2017, с. 128)

Хибридни войни и дезинформация

В съвременния глобализиран свят междудържавните отношения имат водещо място, най-вече по отношение новата среда на сигурност. Защитата на националните интереси, създаваните партньорства, цивилизационните ценности пряко и косвено въздействат върху опитите на опоненти, а в някои случаи и на съюзници, да отстояват суверенните си права и амбиции. (Василев, 2024, с. 11)

В информационната област „заплаха“ е възможна опасност (потенциално или реално съществуваща) за извършване на действие, насочено против обекта на защита (информационни ресурси), нанасящо вреда на собственика или потребителя, изразяваща се в опасност от изкривяване или загуба на информация. (Пак там, с. 15-16)

Понятието „хибридна заплаха“ е легитимирано и навлиза устойчиво в публичното пространство след осъществената от Русия анексия на Крим и намесата ѝ на страната на сепаратистите в Донбас, Украйна. И в двата случая населението в тези региони е „откъснато“ морално от Киев. Във връзка с осъществените от Москва действия и зап- лахи различни експерти в областта на сигурността и отбраната дават множество определения, които имат значителни по своята същност допирни точки. Към настоящия момент обаче единна общоприета дефиниция на понятието „хибридна заплаха“ все още няма. (Пак там, с. 25)

В глобален план все повече интернет се използва като основен канал за манипулирана информация и пропаганда, за създаване на психоза, за привличане на последователи, за подпомагане на терористични организации и пр. Все по-активно се използва киберпространството за открито пропагандиране на радикални идеи, привличане на поддръжници, манипулиране на общественото мнение, отправяне на заплахи, разпространяване на дезинформация. (Велчев, 2024)

Карл фон Клаузевиц посочва, че войната е акт на насилие, който има за цел да накара врага да изпълнява нашата воля. (Клаузевиц, 2001, с. 12)

Насилственото действие на войната се наблюдава както при т.нар. „големи“ войни, така и при съпътстващи конфликти, водени с голяма интензивност и решителност, които по общоприетата представа невинаги са „военни действия“. Сепаратистките акции за заемане на територия, етническото прочистване, кървавите преврати, партизанските движения, въоръжените метежи, войните с използване на наемници, въстанията и прочее са част от един непълен списък на познатите „малки“ войни. Тези войни са водени от враждуващи страни и те невинаги са осъществявани от държавни образувания; някои от тях могат да преливат от една форма в друга, като съхраняват насочеността си. Актовете на война или тероризъм поставят под

съмнение рамката на правата на човека почти до степен, в която изглежда, че тя рухва, а всяко право на човека е засегнато по неблагоприятен начин. (Велчев, 2024)

В доклад от 2011 г. НАТО описва подобни заплахи, посочвайки, че хибридната заплаха е общ термин, обхващащ голямото разнообразие от съществуващи неблагоприятни обстоятелства и действия, като тероризъм, миграция, пиратство, корупция, етнически конфликт и др. Новият елемент е възможността НАТО да се сблъска с адаптивно и систематично използване на такива средства поотделно и в комбинация от противници в преследване на дългосрочни политически цели, за разлика от по-случайното им появяване, водено от съвпадащи фактори. (Пак там)

Една от важните задачи в хибридната война е въздействието върху масовото съзнание на обществото, както и съзнанието и реалните действия на определени държавни и обществени лидери, отговорни за вземането на важни политически решения. Оттук произтича и основната цел на хибридната война – с всички възможни средства и по всякакъв начин силово да се завземе властта в държавата, за да се извърши преразпределение на нейните ресурси, както и преразпределение на социалните роли от новата, поставена власт в интерес на друга държава или група от държави. (Пак там)

Модерната хибридна война може да се изразява в предварително планирани, комбинирани симетрични и асиметричния действия, при които широко се използват информационни и психологически операции. С тяхната помощ могат да бъдат решавани и стратегически задачи. Миксирана по този начин, хибридната война се превръща в инструмент за диверсии, поставяне на димни завеси и пропагандни диполи за подготовка на бойното поле в мирновременния период. Интернет и социалните мрежи играят важна роля в обществените отношения и те могат да се използват за значими по мащаб киберзаплахи. (Пак там)

Същността на тази война са т.нар. „хибридни атаки“, политически, икономически, психологически, киберинформационни способи за въздействие и паравоенни, терористични и криминални методи за контролиране на конфликта. От друга страна, конвенционални военни действия могат да съпътстват или да изпреварват хибридните атаки, или могат да отсъстват, ако преследваните цели са достигнати. (Пак там)

Дезинформацията е невярно или подвеждащо съдържание, което се разпространява с цел заблуда или търсене на икономически или политически ползи.Тя се различава от невярната информация, която представлява невярна или подвеждаща информация, разпространявана без зловредни намерения. (Европейски съвет)

Европейската комисия определя дезинформацията като „създаване, представяне и разпространяване на доказуемо невярна или подвеждаща информация с цел да се извлече икономическа изгода или съзнателно да се въведе в заблуждение

обществеността, което може да бъде в ущърб на обществения интерес“. (Европейска сметна палата)

Определението на Комисията за дезинформация изключва заблуждаващата реклама, съобщаването за грешки, сатирата и пародията, както и ясно разпознаваеми политически мотивирани новини и коментари. За разлика от изказванията, проповядващи омраза, или материалите с терористично съдържание например, невярната или подвеждаща информация сама по себе си не е незаконна. (Пак там)

Стратегическото и координирано разпространение на дезинформация, което попада в обхвата на чуждестранното манипулиране на информация и вмешателство, може да се извършва от държавни или недържавни участници, често като част от поширoки хибридни кампании, с цел манипулиране на информационната среда за извличане на политически ползи, ползи, свързани със сигурността, или други стратегически ползи. (Европейски съвет)

Дезинформацията и чуждестранното манипулиране на информация и вмешателство имат сериозни последици за правата на човека и демократичните ценности. Те застрашават свободата на мисълта, правото на неприкосновеност на личния живот, правото на демократично участие и подкопават доверието на хората в демократичните институции и медии. (Пак там)

Правните аспекти на дезинформацията надхвърлят нейния обхват и са неразривно свързани с въпроси като: регулацията на платформите и тяхната отговорност за съдържанието, предоставено от трети страни и хоствано от тях; противодействието не само на незаконно, но и на вредно съдържание (лъжата не е незаконна) и нуждата да се въведат гаранции, че се спазва принципът незаконното съдържание и онлайн, и офлайн да бъде санкционирано; дали премахването на невярна информация е правилният път; как да се гарантира ефективност на прилагането на законодателните мерки; възможно ли е да се наложат механизми за по-добро управление и самооценка на системите рискове на платформите и дали това ще доведе до ефективни мерки за противодействие на дезинформацията; въвеждане на повече прозрачност по отношение на рекламата и алгоритмите, в частност на тези, свързани с политическата реклама и други. (Юрукова, 2022)

Основният въпрос, свързан с правните аспекти и дезинформацията, е намирането на баланс, защото регулирането не може да бъде достатъчно ефективно за противодействие на неблагоприятните последици от фалшивите новини, без в известна степен да се наложи ограничение на свободата на изразяване. Следователно постигането на подходящ и ефективен баланс между борбата с дезинформацията и зачитането на свободата на изразяване137 е ключовата тема в

дискусиите сред експертите, изследователите и правителствата на държавите по света. (Пак там)

Ролята на основните международни актьори в зашитата на информационната сигурност

В началото на XXI век човечеството е в динамичен рисков етап на развитие, при който международните политически кризи и конфликти са обичайно явление. Предизвикателствата и заплахите вече не са от симетричен и линеен характер, а са предимно асиметрични, нелинейни, мрежови и хибридни. (Василев, 2024, с. 11)

Резултатите от срещите на върха на НАТО в Уелс (2014 г., Великобритания) и на НАТО и Европейския съюз (ЕС) във Варшава (2016 г., Полша) показва, че и двата съюза използват понятието „хибридна заплаха“ като обобщително за определяне на неясни от- крити и прикрити действия на определена държава, която прилага всички инструменти на силата за постигане на специфични политически цели. В техните позиции съществува тенденцията за разполагане на тази заплаха в пространството между законни и незаконни действия и методи, национални и международни правни норми, ред и безредие, информация и пропаганда, традиционни и нетрадиционни средства. (Пак там, 27)

На основата на приетата през 2010 г. от НАТО основополагаща концепция „Военен принос в борбата с хибридните заплахи“ през 2015 г. е създадена „Стратегия за ролята на НАТО за противодействие на хибридната война“, в която хибридните заплахи са определени като „способност едновременно да бъдат адаптивно използвани традици- онни и нетрадиционни средства за постигане на цели“. Те се дефинират и като широк комплекс от прикрити и открити военни, паравоенни и цивилни мерки, организирани в единен модел. (Пак там)

Съгласно заключение на Съвета на Европейския съюз, държавите членки носят основната отговорност за борбата с хибридните заплахи. Усилията на равнище ЕС са взаимно допълващи се по своето естество и не засягат изключителната компетентност на държавите членки по въпросите на националната сигурност. За справяне с хибридните заплахи е необходим всеобхватен подход, който обхваща всички нива на управлението и на обществото, като се работи във всички съответни сектори на политиката по по-стратегически, координиран и съгласуван начин. Важно е подходът, който обхваща всички нива на управлението, да се спазва и да се прилага и на равнище ЕС ЕС и неговите държави членки следва да продължат да развиват, обучават и упражняват способностите за откриване, анализиране на източниците и реагиране на хибридни действия и да подкрепят повишаването на устойчивостта на държавите членки и на институциите, органите и агенциите на ЕС

по отношение на хибридните заплахи в дългосрочен план, като се възползват в пълна степен от съществуващите подходящи за целта инструменти. Съветът изтъква необходимостта от актуализиране на оперативния протокол на ЕС за борба с хибридните заплахи въз основа на извлечените поуки от предишни учения. Съветът подчертава продължаващата необходимост от сътрудничество с международни организации като ООН, ОССЕ, Съвета на Европа и формати като Г-7, за да бъде защитен основаният на правила световен ред, също и в контекста на борбата с хибридните заплахи, включително чрез мерки за изграждане на доверие и други подходящи мерки. (Съвет на Европейския съюз)

Призовава се за непрекъснати и устойчиви усилия за постигане на по-нататъшен напредък в изпълнението на всички действия, свързани с борбата с хибридните заплахи, в рамките на общия набор от предложения за изпълнението на съвместните декларации относно сътрудничеството между ЕС и НАТО, включително в областта на ситуационната осведоменост, стратегическата комуникация, предотвратяването и реакцията на кризи и укрепването на устойчивостта. Във връзка с това Съветът изтъква отново необходимостта от по-нататъшно засилване на политическия диалог относно борбата с хибридните заплахи, както и необходимостта от редовни паралелни и координирани учения (PACE) с участието на всички държави – членки на ЕС, и съюзниците от НАТО, и призовава за своевременно финализиране на новия план за PACE. Съветът изтъква необходимостта да се вземат предвид направените изводи и значението на безпрепятствения обмен на информация по приобщаващ и недискриминационен начин. (Пак там)

Основният проблем е, че не всички страни в НАТО и ЕС оценяват по еднакъв начин хибридните заплахи като основно предизвикателство за сигурността. Наблюдават се различия във вижданията както за същността им, така и за техния източник. Като цяло е възприето, че те идват както от изток (Русия), така и от юг (основно тероризмът, регионалната нестабилност в Близкия изток и Северна Африка, масовата миграция). Разнопосочни обаче са оценките на някои членки относно възприемането на действията на Русия в Европа днес – Балтийските държави, Полша и Румъния ги считат за пряка заплаха за съюзната и национал- ната сигурност, докато Унгария, Словакия, Чехия, Гърция и Кипър смятат това становище за недотам вярно. (Василев, 2024, с. 29)

САЩ определят „хибридната заплаха“ като съчетания от действия на конвенционални въоръжени сили с нередовни сили, които едновременно ангажират и използват наличните им военни способности и средства, подкрепени от комбинация от модерни технологии, конвен- ционални оръжия, кибератаки и информационни операции за постигане на взаимноизгодни политически цели. (Пак там)

Като „хибридни заплахи“ във Великобритания, се класифицират: диверсионни действия на паравоенни формирования (национални самоорганизирани, чуждестранни без опознавателни знаци, наемни и посреднически) на териториите на държавите по южните и източните граници на Алианса; преки киберинформационни и психологически атаки, масирана пропаганда и дезинформация, насочени срещу тези страни; дмонстрация на сила по границите им. (Пак там)

В Република България – на национално ниво липсва доктринално формулирано и законно възприето определение на понятието „хибридна заплаха“, което до известна степен възпрепятства изготвянето на национална стратегия за противодействие. Терминът придобива популярност у нас покрай провокиралия словесна риторика стратегически документ „Визия: България в НАТО и в европейската отбрана 2020“. В него се указва единствено смисълът на понятието „хибридна война“, която „съчетава прилагане на конвенционални методи с похвати от партизанска война, прикрито подпомагане на сепаратистки групировки, кибератаки и пропаганда, икономически натиск и действия, противоречащи на международното право“. (Пак там, с. 30)

Планът за действие на ЕС за борба с дезинформацията е насочен за Подсилване на оперативните групи за стратегическа комуникация и делегациите на ЕС с допълнителни ресурси (човешки и финансови) за откриване, анализиране и разкриване на дейности по дезинформация и преразглеждане на мандатите на оперативните групи за стратегическа комуникация за

Западните Балкани и Южното съседство. (Европейска сметна палата)

Не съществува правна уредба на ЕС в областта на дезинформацията, с изключение на член 11 от Хартата на основните права относно свободата на изразяване на мнение и свободата на информация, както и на поредица от инициативи на политиката. Отговорността за борбата с дезинформацията принадлежи основно на държавите членки съгласно членове 2—6 от Договора за функционирането на Европейския съюз. (Пак там)

Стратегията на ЕС за киберсигурност има за цел да изгради устойчивост на киберзаплахи и да гарантира, че гражданите и предприятията се възползват от надеждни цифрови технологии. (Европейска комисия)

В стратегията се описва как ЕС може да използва и укрепва всички свои инструменти и ресурси, за да бъде технологично независим. В него също така се посочва как ЕС може да засили сътрудничеството си с партньори по света, които споделят нашите ценности за демокрация, върховенство на закона и права на човека. (Пак там)

Технологичният суверенитет на ЕС трябва да се основава на устойчивостта на всички свързани услуги и продукти. Всичките четири киберобщности — тези, които се занимават с вътрешния пазар, с правоприлагането, дипломацията и отбраната — трябва да работят в по-тясно сътрудничество за постигане на общо съзнание за заплахите. Те следва да бъдат готови да реагират колективно, когато се осъществи нападение, така че

ЕС да може да бъде по-голям от сумата на своите части. (Пак там)

Стратегията обхваща сигурността на основни услуги като болници, енергийни мрежи, железопътни линии и все по-големия брой свързани обекти в нашите домове, офиси и фабрики. Стратегията има за цел да изгради колективни способности за реагиране на големи кибератаки. В него също така се очертават планове за работа с партньори по целия свят, за да се гарантира международната сигурност и стабилност в киберпространството. Освен това в него се очертава как съвместно киберзвено може да гарантира най-ефективната реакция на киберзаплахи, като използва колективните ресурси и експертния опит, с които разполагат държавите членки и ЕС. (Пак там)

Новата стратегия има за цел да осигури глобален и отворен интернет със силни предпазни мерки, когато съществуват рискове за сигурността и основните права на хората в Европа. След напредъка, постигнат в рамките на предишните стратегии, в него се съдържат конкретни предложения за разгръщане на три основни инструмента. Тези три инструмента са регулаторни, инвестиционни и политически инициативи. (Пак там)

Общественият аспект на комуникациите в областта на националната отбрана е по-слабо разбирана организационна функция на военните по света. Въпреки че конвенционалните усилия за пропаганда и дипломация датират от векове, съвременният подход към военните стратегически комуникации е неясен и не е добре разбран от обществеността. (Koch, 2024, с. 1)

Заключение

Защитата на информационната инфраструктура е приоритет на основните международни актьори. Комуникационните процеси влияят значителни върху международната сигурност. Все повече нараства необходимостта от допълнително разработване на национални и съюзни политики и стратегии за киберотбрана и сигурност. Включването на кибер пространството като потенциална среда на военно противоборство изисква на неговата защита да се даде висок приоритет. Затова е необходимо държави и международни организации да обединят усилията си и да се противопоставят срещу разпространението на дезинформацията. От съществено

значение е прилагането на сериозни наказания срещу разпространителите на невярна информация с цел манипулация и заплаха на средата за сигурност.

Библиография

Василев, В. (2024) *България във фокуса на хибридните заплахи от Русия.* София: Военна академия „Г. С. Раковски“. [Vasilev, V. (2024) Bulgaria vav fokusa na hibridnite zaplahi ot Rusia. Sofia: Voenna akademia „G. S. Rakovski“.]

Велчев, А. (2024) „Хибридни войни, медии, интернет: основни понятия и пресечни точки“. *Интернет* [онлайн]. ISSN 1314-4464. Достъп: 12.12.2025. Наличен на: https://rhetoric.bg/хибридни-войни-медии-интернет-основн [Velchev, A. (2024) „Hibridni voyni, medii, internet: osnovni ponyatia i presechni tochki“. Internet [onlayn]. ISSN 1314-4464. Dostap: 12.12.2025. Nalichen na: https://rhetoric.bg/hibridni-voyni-medii-internet-osnovn]

Войноховска, В. и Цанков, С. (2014) „Въведение и ключови понятия, свързани с информационната сигурност“. *Научни трудове на Русенския университет*, 53(6.1), 71–76. [Voynohovska, V. i Tsankov, S. (2014) „Vavedenie i klyuchovi ponyatia, svarzani s informatsionnata sigurnost“. Nauchni trudove na Rusenskia universitet, 53(6.1), 71–76.]

Европейска комисия (н.д.) *Стратегия на ЕС за киберсигурност.* [онлайн]. Достъп: 18.12.2025. Наличен на: https://digital-strategy.ec.europa.eu/bg/policies/cybersecurity-strategy [Evropeyska komisia (n.d.) Strategia na ES za kibersigurnost. [onlayn]. Dostap: 18.12.2025. Nalichen na: https://digital-strategy.ec.europa.eu/bg/policies/cybersecurity-strategy]

Европейска сметна палата (2021) *Дезинформация, която засяга ЕС – въпреки предприетите действия, тя все още не е овладяна.* [онлайн]. Достъп: 06.02.2026. Наличен на: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_BG.pdf [Evropeyska smetna palata (2021) Dezinformatsia, koyato zasyaga ES – vapreki predprietite deystvia, tya vse oshte ne e ovladyana. [onlayn]. Dostap: 06.02.2026. Nalichen na: https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_BG.pdf]

Европейски съвет (н.д.) *Дезинформация и демократична устойчивост.* [онлайн]. Достъп: 08.12.2025. Наличен на: https://www.consilium.europa.eu/bg/policies/disinformation-and-democraticresilience/ [Evropeyski savet (n.d.) Dezinformatsia i demokratichna ustoychivost. [onlayn]. Dostap: 08.12.2025. Nalichen na: https://www.consilium.europa.eu/bg/policies/disinformation-and-democraticresilience/]

Европейски съвет (н.д.) *Киберотбрана.* [онлайн]. Достъп: 10.01.2026. Наличен на: https://www.consilium.europa.eu/bg/policies/cyber-defence/ [Evropeyski savet (n.d.) Kiberotbrana. [onlayn]. Dostap: 10.01.2026. Nalichen na: https://www.consilium.europa.eu/bg/policies/cyber-defence/]

Калчев, К. и Цветков, К. (2022) *Киберсигурност.* София: Военна академия „Г. С. Раковски“. [Kalchev, K. i Tsvetkov, K. (2022) Kibersigurnost. Sofia: Voenna akademia „G. S. Rakovski“. []]

Клаузевиц, К. (2001) *Теория на голямата война.* София: Софи-Р. [Klauzevits, K. (2001) Teoria na golyamata voyna. Sofia: Sofi-R.]

Панайотова, М. (2017) *Сигурността и отбраната на ЕС след Лисабонския договор и Стратегическата концепция на НАТО от 2010 г.* София: Институт за икономическа политика. [Panayotova, M. (2017) Sigurnostta i otbranata na ES sled Lisabonskia dogovor i Strategicheskata kontseptsia na NATO ot 2010 g. Sofia: Institut za ikonomicheska politika.]

Слатински, Н. (2011) „Съдържание и измерения на категорията ‘сигурност’“. *Международни отношения*, 4, 89–118. [Slatinski, N. (2011) „Sadarzhanie i izmerenia na kategoriyata ‘sigurnost’“. Mezhdunarodni otnoshenia, 4, 89–118.]

Съвет на Европейския съюз (2019) *Заключения на Съвета относно допълнителните усилия за укрепване на устойчивостта на хибридни заплахи и за борба с тях.* [онлайн]. Достъп: 06.02.2026. Наличен на: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/bg/pdf (data.consilium.europa.eu in Bing)

Уикипедия (н.д.) *Информация.* [онлайн]. Достъп: 07.02.2026. Наличен на: https://bg.wikipedia.org/wiki/Информация [Uikipedia (n.d.) Informatsia. [onlayn]. Dostap: 07.02.2026. Nalichen na: https://bg.wikipedia.org/wiki/Informatsia]

Цветкова, М. (2011) „Внимателна употреба на понятието ‘информация’“. *Интернет* [онлайн]. ISSN 1313-9908. Достъп: 07.02.2026. Наличен на: https://mediajournal.info/education/vnimatelna-upotreba-na-ponyatieto-informacziya/#elementortoc__heading-anchor-1 [Tsvetkova, M. (2011) „Vnimatelna upotreba na ponyatieto ‘informatsia’“. Internet [onlayn]. ISSN 1313-9908. Dostap: 07.02.2026. Nalichen na: https://mediajournal.info/education/vnimatelna-upotreba-na-ponyatieto-informacziya/#elementortoc__heading-anchor-1]

Юрукова, М. (2022) „Дезинформация онлайн: стратегии за противодействие в ЕС“. *Интернет* [онлайн]. Достъп: 08.02.2026. Наличен на: https://digital.libsu.unisofia.bg/bg/v/60144 [Yurukova, M. (2022) „Dezinformatsia onlayn: strategii za protivodeystvie v ES“. Internet [onlayn]. Dostap: 08.02.2026. Nalichen na: https://digital.libsu.unisofia.bg/bg/v/60144]

Buzan, B. and Waever, O. (1998) *Security: A New Framework for Analysis.* Boulder, CO: Lynne Rienner Publishers.

European Union, EUR-Lex (н.д.) *Cybersecurity of network and information systems.* [online]. Accessed: 13.01.2026. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/cybersecurity-of-networkand-information-systems.html

Koch, H. (2024) "Strategic Communications in the Global Security Environment: StratCom's Shift of the Balance of Power." *Internet* [online]. Accessed: 20.11.2025. Available at: https://journals.macewan.ca/muse/article/view/2540

The Impact of Information and Disinformation on the Communication Processes of the International Security Environment

Rositsa Filatova
Sofia University "St. Kliment Ohridski"
ORCID ID: 0000-0002-3496-150X
email: rositsafilatova@gmail.com

Abstract. The report examines various aspects of the impact of information and disinformation on the communication processes of the international security environment. Special attention is paid to defining the concept of security and examining various manifestations of information and disinformation. The role of cybersecurity and the fight against hybrid threats is highlighted. In the international security environment, disinformation is used to mislead and create false impressions. The main task of international actors is to seriously oppose its spread and to create methods that will protect international security.

Keywords: information, disinformation, international security, communication, cybersecurity