

Кибердипломацията – инструмент за комуникация на международни организации

 **Росица Филатова**

Софийски университет „Св. Климент Охридски“
имейл: rositsafilatova@gmail.com

DOI: <https://doi.org/10.58894/AEDV5201>

Резюме. Държави и международни организации имат все повече киберспособности, а необходимостта от използването на „мека сила“ като кибердипломация, играе важна роля за предотвратяване на кибератаки, чрез поддържане на постоянен диалог между партньори и потенциални противници. Кибердипломацията е естествената еволюция на публичната дипломация за включване и използване на иновативните платформи за комуникация през 21-ви век.

Ключови думи: кибердипломация, международни организации, комуникация, киберсигурност, киберпространство

Въведение

Международните организации представляват едновременно цел и рамка на международните отношения и комуникация. Те позволяват намирането на баланс в отношения между основните сили и постигането на равновесието между различните интереси и съставляват рамката, в която се развиват международните отношения, като определят принципите и механизмите на тези отношения. (Шарпантие 2006)

Киберпространството като цяло е интерактивна комуникационна среда, чрез която всеки, който има достъп до нея, може широко и незабавно да разпространява и получава идеи и мнения за конкретни цели. По тази причина киберпространството е признато за важна област с улеснен бърз обмен на информация. (Денчев 2019)

Когато разглеждаме появата на кибердипломацията, е важно първо да разберем основната логика на сътрудничество в тази област. Киберпространството акумулира редица характеристики, които рамкират дипломатическата ангажираност между заинтересованите страни. Като начало, това е глобален домейн, свързващ нации и

граждани по целия свят по различни начини, генерирайки както взаимодействия, така и разногласия между тях. (Денчев 2019)

В медийните и политическите дискусии често чуваме за „кибердипломация“, израз, който съчетава „дипломация“ и „киберсигурност“. Дипломацията е работата, която дипломатите извършват, за да продължат интересите на държавните институции или организации, които представляват, чрез представителство, комуникация и преговори, наред с други процеси. Киберсигурността е набор от мерки, които отделни лица, организации и институции прилагат, за да защитят своите материални активи, например хора, сгради или инфраструктури от кибератаки или нематериални активи например данни, знания, способността да доставят услуга, сила или идеи. (Пак там)

Кибердипломацията е еволюцията на публичната дипломация, за да включи и използва новите платформи за комуникация през 21-ви век. Както обяснява Ян Мелисен в "Новата публична дипломация: мека сила в международните отношения", кибердипломацията "свързва въздействието на иновациите в комуникациите и информационните технологии с дипломацията". (Мелисен 2007) Кибердипломацията е в основата на това, че "признава, че новите комуникационни технологии предлагат нови възможности за взаимодействие с по-широка общественост чрез възприемане на мрежов подход и извличане на максимума от все по-мултицентричната глобална, взаимнозависима система". (Пак там)

Стълбове на кибердипломацията са ясно очертани и са в процес на стабилно изграждане, като централни елементи на мерките за създаване на капацитет и доверие в киберпространството, съгласно насоките на Съвета за сигурност на Организацията на обединените нации, вследствие на което може да синтезираме последващата необходимост от:

- развиване и изграждане на устойчивост на институциите, способни да реагират и да противодействат на киберзаплахи;
- осигуряване на дипломатически ангажменти за поддържане на открито, свободно и безопасно киберпространство;
- изготвяне на правна рамка. (Денчев 2019)

Цел на настоящото изследване е чрез исторически и настоящи примери да се разкрият и обосноват най-значимите аспекти на появата и развитието на кибердипломацията като инструмент на комуникация на основни международни организации, отчитайки

съвременните тенденции на дигитализация и глобализация, които се превръщат отправни точки в международната комуникация.

Тази статия предлага да се изследва концепцията за кибердипломацията, като се анализира нейната еволюция и се свързва с по-широките дискусии за дипломацията като основна институция на международното общество, както е определено от Английската школа за международни отношения. Кибердипломацията е нововъзникваща международна практика, която се опитва да изгради кибер-международно общество, свързвайки националните интереси на държавите с динамиката на световното общество.

Кибердипломация и киберсигурност в ЕС

Киберпространството е нерегулиран терен за злонамерени действия и всички актьори са готови да използват това. Високата степен на анонимност, черните пазари на злонамерен софтуер и недоволството към съществуващите правителства означават, че дори, ако държавите се откажат от кибератаки, хората и отделните групи все още ще имат достъп до техники за атака. Най-добре е да се подготвим именно за това бъдеще. Тъй като нациите няма да се откажат от възможностите за кибератаки, не можем да очакваме да елиминираме използването на такива похвати (дори само защото техниките за кибершпионаж могат лесно и бързо да бъдат адаптирани за атака). Предвид скрития характер на повечето киберпрограми, не можем да предположим, че всяко международно споразумение ще премахне риска от кибератака. В по-късен период може би кибертехнологиите могат да станат сигурни, но тази точка е далечна и дори ако технологията се подобри, противникът винаги може да използва човешката грешка – нещо, което никога няма да изчезне – за да проникне и да атакува. Кибератаката е нещо, с което светът ще трябва да живее, а това означава, че демократичните държави трябва да се съсредоточат върху това как най-добре да управляват и ограничават риска, за да създадат стабилна среда. (Цеков 2019)

Появата на новите информационни технологии, породили сериозни предизвикателства за сигурността на държавите и международни те организации, добави нови участници на масата за преговори относно кибернормите и отговорното поведение в киберпространството. През последните двайсетина години държавите предприеха много опити за постигане на компромис по въпроса за регулиране използването на информационно-комуникационните технологии (ИКТ). Показателно е, че първоначално ИКТ се разглеждаха от гледната точка на новите възможности и иновации за развитие на потенциала на конкретната страна и нейната икономика, при положение, че само малка група държави обръщаше внимание на потенциалните рискове от

злоупотреба с ИКТ за военни цели с цел да бъде ерозиран световният мир и сигурността на планетата. (Стадник 2019)

Стратегията на ЕС за киберсигурност от 2020 г. има за цел да изгради устойчивост на киберзаплахи и да гарантира, че гражданите и предприятията се възползват от надеждни цифрови технологии. Стратегията описва как ЕС може да използва и укрепва всички свои инструменти и ресурси, за да бъде технологично суверенен. В него се посочва също така как ЕС може да засили сътрудничеството си с партньори от цял свят, които споделят нашите ценности за демокрация, върховенство на закона и права на човека. Технологичният суверенитет на ЕС трябва да се основава на устойчивостта на всички свързани услуги и продукти. (Европейска комисия)

Стратегията има за цел да гарантира глобален и отворен интернет със силни гаранции, когато съществуват рискове за сигурността и основните права на хората в Европа. След напредъка, постигнат по предходните стратегии, той съдържа конкретни предложения за използване на три основни инструмента. Тези три инструмента са регулаторни, инвестиционни и политически инициативи. Те разглеждат три области на действие на ЕС:

1. устойчивост, технологичен суверенитет и лидерство;
2. оперативен капацитет за предотвратяване, възпиране и реагиране;
3. сътрудничество за постигане на напредък в глобалното и отворено киберпространство. (Пак там)

Предстоят предизвикателства за кибердипломацията, както е посочено в релевантния инструментариум на ЕС. Обединена Европа има интерес от създаването на стандарти и норми за стабилност и безопасност на киберпространството. Тук са заложили безопасността и стабилността на ЕС, както и влиянието му на международната сцена за сигурност. Дипломатическите мисии на всички страни по света, следва стратегически да разгърнат, амбициозни и координирани действия в областта на киберсигурността. С изключение на най-развитите демократични страни, останалите държави следва да разгърнат своя набор от инструменти за кибердипломация, които в момента са в начален стадий, с помощта на експерти в областта на информационните технологии и дипломати, както и с представители на академичните среди. (Денчев 2019)

По-специално, бъдещото развитие на мерки, които повишават отчетността и отговорността на лицата и образуванията, отговорни за

извършването на кибератаки срещу сигурността, следва да бъде приоритет в изготвянето и разработването на адекватна правна рамка, която да създаде ясни граници и да даде точно определени дефиниции на това какво е кибервойна, киберпрестъпление и кибертероризъм, за да се използва ефективно и адекватно целият арсенал на кибердипломацията. Усъвършенстваният спектър на киберзаплахите трудно може да бъде подреден изчерпателно, но може би основният инструментариум за неговото ефективно противопоставяне е кибердипломацията. С нейна помощ, целта е да се създаде отворено, свободно, стабилно и сигурно реално и киберпространство, което да се регулира от международното право чрез договори и съюзи между държави, организации, съюзи, частният сектор, гражданското общество и експерти. Ясно е, че кибердипломацията е обвързана пряко с направленията за превенция на киберзащитата и киберсигурността. Вниманието на международната общност включва зараждащата се надпревара във въоръжаването и необходимостта от регулиране на режимите за контрол на износа на стоки с двойна употреба и изясняване на правилата за участие в евентуална виртуална и реална кибервойна. (Пак там)

Въпреки експертния си опит в кампании за повишаване на обществената осведоменост в киберпространството, научноизследователска и развойна дейност и образователни програми, ЕС все още е обект на постоянни кибератаки. Отговорът на ЕС на сложния спектър от киберзаплахи е всеобхватен, но може би най-европейският аспект на неговия инструментариум е кибердипломацията. Кибердипломацията има за цел да осигури многостранни споразумения за кибернормите, отговорно държавно и недържавно поведение в киберпространството и ефективно глобално цифрово управление. Целта е да се създаде отворено, свободно, стабилно и сигурно киберпространство, закотвено в международното право чрез съюзи между държави със сходно мислене, организации, частния сектор, гражданското общество и експерти. Офанзивните киберактьори нарастват по разнообразие, изтънченост и брой. Разрушителните технологии, задвижвани от машинно обучение и изкуствен интелект, представляват както рискове, така и възможности за киберзащита: докато атаките вероятно ще се увеличат по сложност и ще направят приписването още по-проблематично, отговорите и защитите ще станат също толкова стабилни. Многостранните киберинициативи са в изобилие, но те се развиват едновременно с нарастващия тласък за суверенитет в дигиталната сфера. Надпреварата за киберпревъзходство, ако бъде оставена без контрол, може да се превърне в по-голям парадокс на сигурността. Инструментариумът на ЕС в областта на кибердипломацията и неговите двустранни и многостранни ангажменти вече допринасят за по-безопасно и по-принципно киберпространство. Нейната

ефективност обаче зависи от истинското европейско и световно сътрудничество за общото кибернетично благо. В крайна сметка амбицията на ЕС да стане по-способен, като стане "стратегически автономен" или "технологично суверенен", също се основава на надеждна киберотбрана и дипломация. (Европейски парламент)

Търсенето на регулаторна рамка за сигурността на киберпространството е предприето от различни участници. На глобално ниво Организацията на обединените нации създаде [група от правителствени експерти](#), за да обсъди "[нормите, правилата и принципите](#)" на отговорното държавно поведение в киберпространството, за да се подобри международната сигурност. На регионално ниво Организацията за сигурност и сътрудничество в Европа (ОССЕ) също наскоро предприе стъпки за идентифициране на [безотговорно поведение в киберпространството](#), което причинява несигурност и нестабилност. Европейският съюз участва активно в тези международни форуми, като развива своите инструменти и влияние в областта на кибердипломацията. Подходът на ЕС към международната кибердипломация се ръководи от принципи, необходимост и амбиция. Това са някои от основните му характеристики. Тя се основава на ангажимента на ЕС към многостранни споразумения и основани на правила заповеди. Тя се основава на съвместен дипломатически отговор срещу кибератаки, които могат да представляват заплаха за ЕС и/или неговите държави членки. Тя е насочена както към превенцията, така и към управлението на инциденти. Кулминацията на стратегията на ЕС за кибердипломация е [инструментариумът на кибердипломацията](#), който позволява на държавите членки на ЕС, да формулират съгласувани и координирани отговори на киберзаплахите и кибератаките. (Европейски институт за публична администрация)

Както става ясно от инструментариума на ЕС за кибердипломация, изразът "кибердипломация" се използва от представителите на държавите от ЕС във връзка с разработването на дипломатически стратегии, които насърчават международното сътрудничество към общ набор от норми. Същият термин обаче кибердипломацията има и друго приложение в контекста на ЕС. Той също така се отнася до поредица от програмни и оперативни действия за борба с киберпрестъпността и свеждане до минимум на риска и въздействието на кибератаките върху хората и основните инфраструктури. (Пак там)

Подходът на ЕС досега е постигнал реализирането на инструменти за координирани действия срещу кибератаки:

1. Разработен първи законодателен пакет за изграждане на по-силна киберсигурност в ЕС. Европейската комисия и върховният представител за политиката на сигурност предложиха [Закона за](#)

[киберсигурността, Директивата относно сигурността на мрежите и информационните системи.](#)

2. Като част от своята стратегия за киберсигурност сега ЕС разработва координиран механизъм за реагиране при кризи.
3. В него се предвижда държавите членки да координират действията си срещу кибератаките.
4. Той попада под шапката на инструментариума на ЕС за кибердипломация, което означава, че ЕС използва външната дипломация като инструмент за вътрешна сигурност.
5. Тя включва мерки в рамките на общата външна политика и политика на сигурност, за да се предотврати ефектът на доминото върху вътрешната сигурност на ЕС и да се допринесе за международната стабилност в киберпространството.
6. Тя насърчава научните изследвания в областта на киберсигурността, за развитието на технологичните способности и експертен опит в тази област, необходими за ограничаване на зависимостта на ЕС от чуждестранни технологии и умения. (Пак там)

НАТО и киберсигурността

В декларацията от срещата на върха в Уелс още през 2014 г. НАТО призна киберпространството за петото бойно поле, а киберсигурността стана основна задача на колективната защита на страните-членки. Прие се Стратегия за отбрана от хибридни атаки, която заявява, че подобни агресивни действия „могат да предизвикат задействане на чл. 5 от договора за колективна отбрана“ на Алианса. С различни вътрешни Решения почти всички страни-членки на Алианса приеха национални стратегии за киберсигурност. В тях киберсигурността се разглежда като неделима част от националната сигурност. В повечето от тези документи киберпространството се разбира, и като място в което се провеждат кибератаки нарушаващи комуникационните системи на противника. (Денчев 2019)

Дискусиите за кибервойната обикновено се ограничават до компютризираните системи и мрежи, които в масовия случай подпомагат електронното управление, поддържат критичната инфраструктура, доставката на електроенергия, транспорта, финансовите транзакции и т.н. Конфликтът в Украйна обаче показва, че интернет пространството може да играе роля и в провеждането на информационни и психологически операции, където основните цели не са машините или мрежите, а умовете на хората. Произтичащите рискове и заплахи за националната сигурност на страните от Алианса

са очертани в техните национални отбранителни стратегии и в годишните им доклади за състоянието на сигурността, в които се посочва, че през последните години са налице интензивни външни опити за разширяване сферата на влияние в икономическото, културното и информационното пространство на Северно-атлантическия съюз. На първо място уязвимостта на демократичните общества се дължи на това, че до настоящия момент националните им правителства и техните специализирани институции не са предприели защитни или ответни действия за реакция на информационните операции в интернет пространство на Алианса. (Пак там)

Докато либералният международен ред даде възможност за развитието на киберпространството, преминаването към постлиберален ред доведе до появата на кибердипломатията, т.е. използването на дипломатически ресурси и изпълнението на дипломатически функции за защита на националните интереси в киберпространството. Ролята на дипломатията в киберпространството е много по-малко забележима в медиите, отколкото историите за киберинцидентите например. Въпреки че международните различия по отношение на регулирането на интернет могат да бъдат проследени до 90-те години на миналия век, сега те са по-интензивни от всякога. (Пак там)

Киберпространството се превърна в основен фокус на международните отношения. Повечето световни сили вече рационализираха киберпроблемите във външната си политика, приемайки киберстратегии и назначавайки определени дипломати, които да преследват тези стратегически цели.

Киберзаплахите за сигурността на Алианса са сложни, разрушителни и принудителни и стават все по-чести. НАТО ще продължи да се адаптира към развиващия се пейзаж на киберзаплахите. НАТО и неговите съюзници разчитат на силна и устойчива киберотбрана, за да изпълнят основните задачи на Алианса за колективна отбрана, управление на кризи и кооперативна сигурност. Алиансът трябва да бъде подготвен да защитава своите мрежи и операции срещу нарастващата сложност на киберзаплахите, пред които е изправен.

Киберсигурността и киберотбраната са част от основната задача на НАТО за колективна отбрана. Съюзниците от НАТО потвърждават, че международното право се прилага в киберпространството. Основният фокус на НАТО в киберотбраната е да защитава собствените си мрежи, да работи в киберпространството (включително чрез операциите и мисиите на Алианса), да помага на съюзниците да повишат националната си устойчивост и да предоставя платформа за политически консултации и колективни действия. През юли 2016 г. съюзниците потвърдиха отбранителния мандат на НАТО и признаха

киберпространството като област на операции, в които НАТО трябва да се защитава толкова ефективно, колкото и във въздуха, на сушата и в морето. Съюзниците също така поемат обещание за киберотбрана през юли 2016 г., за да подобрят киберзащитата си и продължиха да укрепват националната си устойчивост като приоритет. НАТО засилва киберспособностите си, включително чрез образование, обучение и учения. Съюзниците се ангажират да засилят обмена на информация и взаимопомощта за предотвратяване, смекчаване и възстановяване от кибератаки. Екипите на НАТО за кибер бързо реагиране са в готовност 24 часа в денонощието, за да помогнат на съюзниците, ако бъдат поискани и одобрени. На срещата на върха на НАТО през 2018 г. в Брюксел съюзниците се съгласиха да създадат Център за операции в киберпространството като част от засилената командна структура на НАТО. Те също така се съгласиха, че НАТО може да се възползва от националните киберспособности за операции и мисии. През февруари 2019 г. съюзниците одобриха ръководство на НАТО, което определя редица инструменти за по-нататъшно укрепване на способността на НАТО да реагира на значителни злонамерени кумулативни кибер дейности. НАТО и Европейският съюз (ЕС) си сътрудничат чрез техническо споразумение за киберотбрана, подписано през февруари 2016 г. В светлината на общите предизвикателства НАТО и ЕС засилват сътрудничеството си в областта на киберотбраната, по-специално в областта на обмена на информация, обучението, научните изследвания и ученията. НАТО засилва сътрудничеството си с индустрията чрез Индустриалното киберпартньорство на НАТО. На срещата на върха на НАТО през 2021 г. в Брюксел съюзниците одобриха нова всеобхватна политика за киберотбрана, която подкрепя основните задачи на НАТО и цялостната позиция за възпиране и отбрана, за да се повиши още повече устойчивостта на Алианса. Съюзниците използват НАТО като платформа за политически консултации, споделят опасения за злонамерени кибер дейности и обмен на национални подходи и отговори, както и обмислят възможни колективни отговори. Съюзниците насърчават свободно, отворено, мирно и сигурно киберпространство и полагат усилия за повишаване на стабилността и намаляване на риска от конфликти чрез подкрепа на международното право и доброволните норми за отговорно държавно поведение в киберпространството. (НАТО)

Насоки на ООН в киберпространството

Работна група е създадена от генералния секретар на ООН като част от неговата по-широка [пътна карта за финансиране на Програмата до 2030 г. за устойчиво развитие: 2019-2021 г.](#) Тя трябва да катализира и препоръча начини за използване на цифровото финансиране, за да се ускори финансирането на целите за устойчиво развитие. Тя събра 17 лидери от областта на финансите, технологиите, политиката, регулирането и международното развитие, които чрез съвместната си

работа се ангажираха в десетки страни и със стотици експерти и институции. (ООН)

ООН подкрепя държавите членки в изпълнението на Програмата до 2030 г. за устойчиво развитие. Като част от това има три начина, по които ООН може да придвижи напред програмата за действие на работната група:

- Чрез постигане на напредък в приведените в съответствие с устойчивостта решения за цифрово финансиране на национално и регионално равнище.
- Чрез изграждане на приобщаващо международно управление, насочено по-специално към постигане на напредък в прилагането на подходящи принципи на управление и по-приобщаващо разработване на политики и регулаторни разпоредби.
- Като илюстрира добрите практики в областта на прозрачността и отчетността на собствените си финанси, включително тези, които насочва към дейности в държавите членки. (Пак там)

Въпреки скептицизма и продължаващото геополитическо напрежение, държавите-членки на ООН постигат консенсус да одобрят доклад на Отворената работна група на ООН за киберсигурност от 2021 г., съдържащ препоръки за постигане на мир и сигурност в киберпространството. Докладът не е правно обвързващ, нито новаторски в съдържанието си, но отбелязва първия път, когато процес, отворен за всички страни, води до споразумение за международна киберсигурност. (Съвет за външни отношения)

Докладът като цяло отразява точките на консенсус и също така прави препоръки за по-нататъшен напредък в областта на възникващите заплахи, доброволните поведенчески норми, международното право, изграждането на капацитет, мерките за изграждане на доверие и потенциалните формати за редовен диалог на ООН по тези теми. (Пак там.)

Успехът на Отворената работна група на ООН за киберсигурност в постигането на консенсус означава, че международната сигурност в киберпространството за първи път се превърна в въпрос, който се обсъжда от всички държави-членки на ООН. (Пак там)

Заклучение

Въпреки че дипломатическите практики са се развили значително, литературата изненадващо остава ограничена, създавайки нова пропаст между практиката и теорията. Има многобройни статии за

киберполитиките, разработени от конкретни страни, за отношенията между определени държави или за специфични аспекти на международните отношения в киберпространството. Проучванията, фокусирани върху конкурентните визии за управление на интернет, са доста многобройни. И все пак има много ограничени усилия за дефиниране или концептуализиране на кибердипломацията и за разбиране как дипломатите и чуждестранните служби поемат отговорността за тези сравнително нови въпроси. Повече яснота относно определението и целите на кибердипломацията би била полезна за тези, които я практикуват, докато литературата за дипломацията и международната политика може да се възползва от ретроспекцията от нова област на политиката.

Основната разлика на кибердипломацията в сравнение с други форми на дипломация е, че тя е сравнително нова област на конкуренция и сътрудничество между държавите, където правилата, нормите и ефектите от действия или бездействия на държавите не са ясно определени. Тези, които се ангажират на дипломатическо ниво по кибервъпроси, трябва да разработят рамка за ангажиране в кратък период от време, без възможност за използване на рамки от други области като ръководство. (Атлантически съвет)

Бързата дигитализация увеличава кибератаката с темпове, които не са съчетани с усилията за нейното осигуряване или от международната общност като цяло, демонстрираща отговорно поведение в киберпространството, така че дипломатическата общност е оставена да се бори с тези въпроси.

Тъй като технологиите стават все по-важни, различни дискусии за кибердипломацията са забележителни, тъй като те се стремят да изградят нормативна рамка за киберпространството. Тази рамка е значима и последователна – нейният регулаторен избор носи икономически, политически, социални и защитни последици за отделните държави и международната общност като цяло.

Кибердипломацията по същество прилага дипломатически инструмент, насочен към киберпредизвикателствата, и обхваща: изграждане на съюзи и колективен отговор на киберзаплахите; договаряне на рамка за киберстабилност, която включва правила за пътя за действия на държавата в киберпространството; договаряне на двустранни споразумения и рамки за сътрудничество; гарантиране на спазването на правата на човека в киберпространството; използване на дипломатически инструменти за реагиране на заплахи. (Пак там)

Нормите и международното право са базова линия на приемливо държавно поведение в киберпространството. Без тях това би било беззаконно пространство. Дори когато държавите нарушават

договорените норми, те осигуряват сплотяваща точка за други държави, за да изискват спазване и да насърчават отчетността.

Има правила във всички аспекти на живота ни, които ни позволяват да функционираме като общество. Няма причина киберпространството да е по-различно. В допълнение към договорените норми, международното право, международното хуманитарно право и правото в областта на правата на човека уреждат какъв тип действия могат да предприемат държавите в киберпространството.

Ако дипломатията е преди всичко междудържавна дейност, дигиталното пространство е създадено и се управлява от недържавни участници, които са пряко засегнати от дейностите на държавите. По този начин постигането на мир и сигурност в цифровото пространство няма да бъде възможно без недържавни участници, което изисква дискусия между тези две категории участници. (Пак там)

Решението на една организация да отдели ресурси за кибердипломатия може да се основава на много фактори, точно както в други области на политиката. Повишената ангажираност може да бъде обусловена от интереса на хората към лидерски позиции. Тя може да бъде стимулирана от инцидент с киберсигурността, който засяга определена компания, сектор, сегмент от обществото или държава и т.н. Тя може да произтича от координиран натиск на гражданското общество по определена тема. Държавите, частният сектор и гражданското общество признават, че голяма част от бъдещия просперитет се крие в киберпространството и че решенията, взети в множество глобални и регионални форуми, ще помогнат за оформянето на бъдещето на киберпространството и как реагираме на заплахите. (Пак там)

Организациите и правителствата, които вървят по пътя на ангажираността на множество заинтересовани страни по кибернетични въпроси, имат потенциала да представят цялостна стратегия за ангажиране, която не пропуска никакви заинтересовани страни и взема предвид всички акции, които могат да бъдат засегнати или повлияни от резултата от дипломатическия ангажимент. Освен това организациите, които имат практически подходи към дипломатията, които успяват да свържат дипломатическото с практиката, имат някои успехи в тази област. (Пак там)

БИБЛИОГРАФИЯ

Денчев 2019: Денчев, С. *Информация и сигурност*. София: За буквите, 2019.

Денчев 2019: Денчев, С. Кибердипломацията – необходимата нова подредба на старите политически бардаци. 2019 . https://nacionalnaisigurnost.bg/sdm_downloads/cyber-diplomacy/

Мелисен 2007: Melissen, Jan. *The New Public Diplomacy: Soft Power in International Relations*. California: Palgrave Macmillan, 2007

Стадник 2019: Стадник, И. Новата кибердипломация. 20.05.2019. <https://www.geopolitica.eu/2019/175-broy-2-2019/3000-novata-kiberdiplomatsiya>

Цеков 2019: Цеков, И. Анализ: Кибердипломацията – между възможното и желаното. 26.11.2019. <https://cedr.bg/%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B4%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC%D0%B0%D1%86%D0%B8%D1%8F%D1%82%D0%B0-%D0%BC%D0%B5%D0%B6%D0%B4%D1%83-%D0%B2%D1%8A%D0%B7%D0%BC/>

Шарпантие 2006: Шарпантие, Ж. *Международните организации*. София, 2006.

Европейска комисия Стратегия за киберсигурност, <https://digital-strategy.ec.europa.eu/bg/policies/cybersecurity-strategy>, последен достъп: 04.02.2023 г.

Atlantic Council The future of cyber diplomacy, <https://www.atlanticcouncil.org/commentary/the-5x5-the-future-of-cyber-diplomacy/> 12.03.2023 г.

Council on foreign relations Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What? <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what> 19.02.2023 г.

European institute of public administration EU Cyber Diplomacy, <https://www.eipa.eu/blog/eu-cyber-diplomacy-101/> 25.02.2023 г.

European parliament Understanding the EU's approach to cyber diplomacy and cyber defence, [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)651937](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651937) 25.02.2203 г.

NATO Cyber defence, https://www.nato.int/cps/en/natohq/topics_78170.htm 25.02.2023 г.

OOH Digital Financing Task Force,
read://https_www.un.org/?url=https%3A%2F%2Fwww.un.org%2Fen%2F
digital-financing-taskforce 19.02.2023 г.

Council on foreign relations Unexpectedly, All UN Countries Agreed on
a Cybersecurity Report. So What?

<https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what> 19.02.2023 г.

Cyber diplomacy – a communication tool of international organizations

 Rositsa Filatova

Sofia University "St. Kliment Ohridski"
email: rositsafilatova@gmail.com

Abstract. States and international organizations increasingly have cyber capabilities, and the need to use "soft power" such as cyber diplomacy plays an important role in preventing cyberattacks by maintaining a constant dialogue between partners and potential opponents. Cyber diplomacy is the natural evolution of public diplomacy to incorporate and use innovative communication platforms in the 21st century.

Keywords: cyber diplomacy, international organizations, communication, cyber security, cyberspace

ФОНД „НАУЧНИ ИЗСЛЕДВАНИЯ“

Броят на тема: „Копирайтинг: медии и маркетинг“ се осъществява с подкрепата на проект (Договор № КП-06-НП4/17 от 01.12.2022 г.), одобрен в конкурсната сесия „Българска научна периодика – 2023 г.“ при Фонд „Научни изследвания“ за издаване на рецензираното научно издание „Медии и език“.