ОЦЕНЯВАНЕ НА ЕТИЧНОСТТА НА КИБЕР АТАКИ КАТО ЕЛЕМЕНТИ НА ХИБРИДНАТА ВОЙНА

ГЕОРГИЕВ Венелин, проф. д-р,
Нов български университет

GEORGIEV Venelin, Prof. PhD,
New Bulgarian University

***Резюме*:** Хибридната война се превърна в съвременна, модерна концепция за противопоставяне, в съдържанието на която се включват кибертаките. Последните по своята същност в повечето случаи се незаконни, но едновременно с това е важно да се отчита спазването на етични правила на противоборството в киберпространството. В доклада се прави преглед на съществуващи рамки от критерии за оценяване етичността на кибератаки и на възможностите за тяхното приложение на базата на нормите от международното право.

***Ключови думи*:** хибридна война, кибератака, етика, международно хуманитарно право, етика на правото за използване на сила, етика на начина за използване на сила.

Abstract: Hybrid war has become a modern concept of opposition, the contents of which include cyber attacks. The cyber attacks are in most cases illegal, but at the same time it is important to take into account the observance of the ethical rules of cybercrime. The report examines existing frameworks of criteria for assessing the ethics of cyber attacks and the possibilities for their application on the basis of the rules of international law.

Keywords: hybrid war, cyber attack, ethics, international humanitarian law, ethics of the right to use force, ethics of the use of force.

„Върховното превъзходство е да покориш врага, без да се сражаваш"
Сун Дзъ

Хибридната война като термин се появява в края на XX век за означаване на нестандартна военна стратегия, включваща и обединяваща в себе си бойни действия, диверсия и кибервойна. Хибридната война не се обявява официално и не се води от регламентирани участници. Прилагането на т.нар. хибридни техники не е ново явление. Засилване на интензивността на използване на подобни техники се наблюдава след края на Студената война.

Хибридната война, чиято концепция представлява естествена еволюция на войната, към момента представлява

най-модерната форма на военен конфликт.

Тя се характеризира с предварително планирани на стратегическо ниво комбинирани симетрични и асиметрични действия с широко използване на информационни и психологически операции. Участниците в хибридната война се стремят да останат неясни и неразпознати при преследване на техните цели като се опитват да запазят въздействието под ниво, което не предизвиква ясно нарушаване на международни норми и предназващо от координирана реакция на международната общност, т.е. при избягване по възможност за пряка военна конфронтация[1].

[1] *Димов Н., Ж. Желев. Хибридната война като част от общата теория на войната. https://postvai.com/analizi/хибридна-война.html*

Сред методите на хибридната война, имащи отношение към настоящата тема, следва да бъдат посочени:

- масово използване на кибератаки;
- провеждане на информационни операции;
- провеждане на психологически операции;
- интензивно технологично противопоставяне;
- водене на поведенческа война.

Успоредно с това интерес представляват и следните характеристики на хибридната война:

- глобален характер, т.е. хибридната война се води навсякъде по света, като при нея в следствие на използването на информационните технологии и компютърните мрежи отпадат неудобствата на географските и физическите граници;
- постоянен и универсален характер от гледна точка на използваните традиционни и нетрадиционни стратегии;
- дифузионен характер, изразяващ се във взаимно проникване на организационна, технологична и информационна среда.

Съществен компонент в разбирането и съдържанието на хибридните войни представляват кибератаките. В едни от случаите тези кибератаки попадат в групата на престъпленията, тъй като включват дейности, инкриминирани в националните законодателства на страните. За този тип кибератаки освен всичко друго е налице нарушаване на етичните норми. За настоящия материал интерес представляват онези кибератаки, използвани в хода на хибридната война, които включват действия, които не са инкриминирани, т.е. които не представляват престъпления, но за които си заслужава да бъде оценявана степента на тяхната етичност. При този тип кибератаки, и по-точно при оценяване на тяхната етичност, може да бъде направено още едно разделение – оценяване на етичността по отношение на правото за използване на сила и оценяване на етичността по отношение на начина на използване на силата.

По отношение на своята етичност не всички кибератаки са равнозначни. Ефектът от кибератака, която спира достъпа до уеб сайт с новини за един час ще бъде сравнително малък в сравнение с тази, която възпрепятства контрола на въздушното движение и причинява сблъсък на самолети. Всъщност, в последния случай последиците са съпоставими с прилагането на сила, в следствие на която са свалени самолетите. Двата примера илюстрират, че по-важното е не толкова да се даде еднозначен отговор на въпроса дали конкретните кибератаки са етични или не, а по-скоро

да се създаде рамка за оценяване на дадена кибератака или клас от кибератаки от гледна точка на тяхната етичност.

Като критерий за оценяване на етичността на кибератаките може да се използва видът на прилаганата сила – „твърда“ или „мека“, както и видът на силата, с която може да се отговори на извършена подобна кибератака.

В Хартата на Организацията на обединените нации (ООН) се определят условията, при които държавите-членки могат да прилагат сила срещу други държави. Най-важните части на Хартата са членове 2 (4), 39 и 51.

Член 2 (4) забранява използването на сила срещу други държави: *Всички държави-членки следва да се въздържат в международните си отношения от заплахата с, или използването на сила срещу териториалната цялост или политическата независимост на*

всяка държава, или по някакъв друг начин, несъвместим с целите на ООН.

Тъй като естеството на тази сила е оставено неизяснено, тук може да бъдат включени не само въоръжените сили, както се визира в другите части на Хартата, където те изрично са адресирани, но и силите и средствата, които се използват в рамките на кибератаки.

Член 39 възлага на Съвета за сигурност на ООН отговорността за отговор при заплахи и актове на агресия: *Съветът за сигурност определя наличието на всяка заплаха за мира, нарушаване на мира или акт на агресия и прави препоръки или решава какви мерки ще бъдат предприети за да се запазят или възстановят международния мир и сигурност.*

Въпреки широката гама от актове, които може да се тълкуват като "заплаха за мира", терминът "агресия" е дефиниран в резолюция на Общото събрание на ООН като "използване на въоръжена сила" („твърда“ сила) от член или не-член на ООН. Тя включва нашествия, атаки, бомбардировки, както и блокади от страна на въоръжени военни сили и други групи, включително наемници.

Член 41 се отнася до отговорите със средства, различни от въоръжените сили, например, "пълно или частично прекъсване на икономическите отношения и средства за комуникация, както и скъсване на дипломатическите отношения", т.е. до отговори с помощта на т.нар. „мека“ сила.

Въпреки, че член 2(4) забранява на държавите да предприемат агресивни действия, член 51 признава правото на самозащита срещу въоръжени атаки:

Нищо в настоящата Харта не може да попречи на прилагането на неотменимото право на индивидуална или колективна самоотбрана, ако съществува въоръжено нападение срещу член на ООН, докато Съветът за сигурност предприеме необходимите мерки за поддържане на международния мир и сигурност. Мерките, предприети от държавите при упражняването на това право на самоотбрана трябва да бъдат незабавно докладвани на Съвета за сигурност и по никакъв начин не бива да повлияват на правомощията и отговорностите на Съвета за сигурност, произтичащи от настоящия устав, за да предприеме по всяко време такива действия, каквито счита за необходими, за да се запазят или възстановят международния мир и сигурност.

Въпреки че член 51 гласи, че защитните мерки, включително използването на сила, са допустими след като дадена държава е била атакувана, то обикновено се разбира, че държавите имат право на "изпреварващи действия за самоотбрана", което означава, че може да се предприемат изпреварващи действия за да се парира атака от страна на опонента. Разрешено е също и да се упражнява "самозащита на неутрална територия". Това означава, че страните могат да използват сила срещу заплахата от територията на неутрална държава, когато тази държава не желае или не може да предотврати използването на нейната територия като база или източник на атаките срещу застрашената държава (DoD OGC, 1999 г., стр. 14.).

В обобщение, Хартата на ООН забранява на държавите-членки използването на сила срещу други държави (член 2 (4)), с изключение на самозащита (член 51) или под егидата на Съвета за сигурност (член 39). Хартата ефективно използва етичния принцип на справедливата кауза за атакуването на друга държава, който повечето хора биха приели. Държавите-членки имат моралното право да се защитават срещу актове и заплахи за агресия, но нямат право да участват в непровокирана агресия (да провокират агресия). Използването на сила е допустимо само като средство за защита срещу агресия.

С цел прилагането на тези правни и етични принципи при кибератака, първо трябва да се определи дали кибератаките представляват използване на „твърда“ или „мека“ сила. В случай че сравнението показва наличие на признаци за използване на „твърда“ сила,

съответните кибератаки ще попаднат в обхвата на Хартата на ООН, заедно с използване на въоръжена сила, което означава, че подобни кибератаки ще бъдат оправдани само като средство за самозащита. Но ако те не се считат за форма на използване на „твърда" сила, етичните въпроси, свързани с тяхното прилагане са по-неясни, попадащи по-близо до обхвата на "меките" форми на принуда, като търговски ограничения и скъсване на дипломатическите отношения.

За целите на изследването по темата е направен преглед на съществуващите в литературата модели на системи от критерии за оценяване на етичността на кибератаки с помощта на приетия в настоящи материал критерии за етичност. В резултат на проведеното изследване са открити и по-надолу описани примери за съществуващи подобни рамки от критерии за оценяване.

На първо място е направен

преглед на съществуващи системи от критерии,

които да позволяват оценяването на етичността на кибератаки от гледна точка на допустимостта за използване на „твърда" или „мека" сила при тяхното провеждане, както и при отговора срещу тях.

Един от примерите за система от критерии за оценяване на етичността на кибератаки е с автор Михаел Шмит, професор по международно право и директор на Програмата за академични изследвания по сигурността в George G. Marshall - Европейският център за изследване на сигурността в Германия. В своята разработка той предлага седем критерия за разграничаване на кибератаки, които използват или които позволяват отговор с „твърда" сила от тези с икономически, дипломатически и други „меки" мерки. За всеки критерий авторът предлага спектър от последствия, като най-високо са поставени тези, които се свързват с използването на „твърда" сила, а в низходящ порядък са тези с „меките" мерки[2].

Тежест на последствията. Тук се включват последствия с убити или ранени хора и материални щети. Предпоставката е, че въоръжените атаки, които използват „твърда" сила често причиняват жертви или материални щети, докато при „меките" мерки това не се наблюдава.

Време на проявление. Това е времето, необходимо за последиците от една операция да влязат в сила. Като общо правило, въоръжени нападения, които използват „твърда" сила имат непосредствен ефект, от порядъка на няколко секунди до минути, докато „меките" мерки, като търговски и икономически ограничения, могат да се проявят в продължение на седмици, месеци, дори години.

Взаимовръзка. Това е връзката между операцията и нейните ефекти. За въоръженото нападение ефектите обикновено са причинени от и се отнасят до прилагането на „твърда" сила, докато за „меките" мерки ефектът може да има няколко обяснения.

Инвазивност. Отнася се до това дали при дадена операция се преминава границата на целевата страна. Като цяло, въоръжено нападение пресича физически граници, докато „меките" мерки се изпълняват в рамките на границите на потърпевшата страна.

Измеримост. Това е възможността да се измерят ефектите от операцията. Предпоставката е, че последиците от въоръжените атаки са по-лесно количествено измерими (брой жертви, стойност на повреденото имущество), отколкото при „меките" мерки (например – измерване на състоянието на дипломатическите отношения).

[2] *Diane Bailey. Cyber Ethics. The Rosen Publishing Group, 2008*

Легитимност. Отнася се до това дали дадена операция се смята за законна в рамките на международната общност. Има се предвид, че използването на въоръжена „твърда" сила по принцип е незаконно при отсъствие на някаква основателна причина, като самоотбрана, докато използването на меките мерки като цяло са законни.

Отговорност. Отнася се до степента, в която резултатът от действието може да се отнесе до дадена държава. Предпоставката е, че въоръжената принуда е в обхвата на правомощията на държавите и е по-вероятно за такива дейности да се държи сметка на държавите, докато недържавните актьори са способни да извършват подобни дейности в обхвата на „меките" мерки като пропаганда и бойкоти.

За да се илюстрира как може да се приложи описаната по-горе система от критерии се използва пример с кибератака на център за управление на полетите, довела до сблъсък на два големи транспортни самолета и петстотин жертви.

Тежест на последствията. Очевидно степента на последствията е много висока. Последствията от кибератаката са съизмерими с тези при атака на двата самолета с ракети от типа „въздух-въздух", т.е. може да се каже, че е налице използване на твърда сила.

Време на проявление. Също висока степен, въпреки лекото закъснение между атаката и проявлението на ефекта (сравнено с една ракетна атака например).

Взаимовръзка. Висок ранг – причината за катастрофата е ясно доказана от информацията на радарите и черните кутии на двата самолета.

Инвазивност. Среден ранг поради виртуалния характер на атаката, не е нужно физическо пресичане на граници.

Измеримост. Много висок ранг – последствията от кибератаката лесно се определят с помощта на броя на жертвите и разрушаването на два граждански самолета.

Легитимност. Висок ранг – напълно нелегитимен акт.

Отговорност. От среден до висок ранг – принципно извършителят може да е всеки, но уменията и необходимите знания изключват повечето хакери, предполагайки държавна поръчка.

В заключение, пет от критериите, включени в рамката за оценяване на етичността на кибератаката, са с висок ранг и два с най-малко среден ранг. Тази атака може да се класифицира като употреба на сила и това дава основание за легитимен силов отговор. По отношение на етичността оценката е, че кибератаката без съмнение не отговаря на общоприетите норми за поведение, т.е. тя категорично е неетична.

За сравнение, една масивна атака от типа отказ от услуга срещу правителствен уеб сайт, използваща стотици компютри-зомби, блокираща достъпа до сайта за един ден би могла да бъде класифицирана на базата на същите критерии по следния начин:

Тежест на последствията. Нисък до среден ранг.

Време на проявление. Висок ранг.

Взаимовръзка. Среден до висок ранг – причината е ясно доказана от логовете.

Инвазивност. Среден ранг поради виртуалния характер на атаката.

Измеримост. Висок ранг – лесно определяне на времето, за което атакувания сървър няма да работи.

Легитимност. Висок ранг – напълно нелегитимен акт, нарушение на закона.

Отговорност. От нисък до среден ранг – принципно извършителят може да е всеки хакер.

В заключение, тази кибератака може да се класифицира като атака с по-незначителна употреба на „твърда" сила и по-скоро като кибератака с „мека" сила.

На базата на представената рамка от седем критерия на професор Шмит, друг учен - Уингфийлд, предлага оценяването на кибератаките по избраните критерии да става с помощта на точкуване по скала от 0 до 10, като високият резултат е в случай на употреба на „твърда" сила, а ниският – за т.нар. „меки" мерки[3].

На второ място в изследването са анализирани

системи от критерии за оценяване на етичността на кибератаки от гледна точка на начина, по който са използвани инструменти съответно на „твърдата" и „меката" сила.

В този случай правният и етичен въпрос относно кибератаката не е дали тя изглежда като употреба на сила, а дали авторът на атаката и съответно авторът на отговора срещу нея се придържат към общоприетите етични принципи. Тези принципи са заложени в различни договори, включително в Хагските регламенти и Женевската конвенция, както и в традиционното международно право.

При направеното търсене се установи, че Министерство на отбраната на САЩ в своята практика използва подобна рамка, обобщена в следните седем принципа: (DoD OGC)[4]:

1) *Разграничаване на военните от цивилните участници в конфликта.* Етиката изисква само членове на редовните въоръжени сили на една нация да могат да използват сила като при това те трябва да могат да бъдат разграничени от цивилните граждани (по униформа, знаци и т.н.), а също така и да не се прикриват зад цивилни граждани или тяхна собственост.

2) *Военна принадлежност.* Целите на атаката трябва да имат директен принос към военните действия или да способстват за постигане на военно предимство.

3) *Пропорционалност.* При атакуване на законна военна цел, съпътстващите щети на цивилните и тяхната собственост трябва да бъдат пропорционални на потенциалното военно превъзходство.

4) *Неприцелни оръжия.* Оръжия, които не могат да бъдат насочени с точност, като например бактериологичните оръжия, не трябва да се използват.

5) *Непоправими последствия.* Не трябва да се използват оръжия, които причиняват катастрофални последствия и нелечими травми (като пример, противопехотни мини).

6) *Коварство.* Защитени символи не трябва да се използват за прикриване на военни цели от атака, както и да се симулира предаване или излъчване на фалшиви съобщения за прекратяване на огъня.

7) *Неутралитет.* Държавите имат право на имунитет срещу атаки, ако те не съдействат по никакъв начин на една от двете воюващи страни. В противен случай те стават законни цели.

Първите три принципи, изброени по-горе, по същество твърдят, че войните трябва да се водят от военни сили и че атаките, независимо дали кинетични или кибер, трябва да бъдат насочени към военни цели, а не към цивилни такива. В този смисъл, кибератаки срещу критични инфраструктури като цивилни енергийни центрове, телекомуникации, транспортни и финансови системи и т.н. са разрешени само ако те не причиняват ненужни или непропорционални съпътстващи щети на цивилни граждани и тяхната собственост.

Първият принцип също така казва, че военните сили трябва да се идентифицират когато извършват атаки, като по този начин поемат отговорност за своите действия. Прилагането на този принцип в киберпространството означава, че кибервойниците не трябва да атакуват

[3] Георгиев Венелин. Човешкият фактор в киберсигурността. Авангард, 2016
[4] Diane Bailey. Cyber Ethics. The Rosen Publishing Group, 2008

анонимно по начин, който да оставя открита възможността, че те работят като цивилни, или от името на друга държава. Тъй като повечето атаки се провеждат така, че да се избегне припознаване и осигуряване на анонимност, постигането на тази цел ще изисква нови средства и методи, например, кибероръжия и атаки, които носят правителствено лого или "знаме", или са ясно проследими. Още по-важно е, че това ще изиска да се постигне промяна в схващането, че кибератаките са непременно тайни операции, които благоприятстват военните операции. Правителствата биха се противопоставили на това, тъй като това ще ги направи по-уязвими на контраатаки.

Въпреки, че компютърните проникванията и атаки от типа „отказ на услуга" могат да бъдат прецизно насочени, някои кибероръжия могат да бъдат забранени на основание на четвъртия принцип - неприцелност. Повечето зловреден софтуер под формата на вируси и червеи попада в тази категория, тъй като те са предназначени да се разпространяват във всяка уязвима машина, в която попаднат. Вирусите и червеите все пак могат да бъдат използвани, но ще трябва да бъдат кодирани по начин, който ограничава тяхното разпространение до целевата подмрежа.

За сега кибероръжия, причиняващи непоправими последствия все още не са налични, но може да си представим кибератака, която е предизвикала такъв ефект чрез промяна на поведението на хирургически робот по време на операция.

За извършване на коварство в киберпространството има достатъчно възможности – скриване на троянски коне във фалшив уеб сайт, носещ емблемата на Червения кръст или поставяне от издирван терорист на фалшиво известие за предаване на уеб сайтове, използвани от него за разпространяване на съобщения. Съгласно изброените по-горе принципи такива действия не са разрешени и влизат в конфликт с етиката на кибератаките.

Принципът на неутралност защитава неутралните държави от атака. За илюстрация, ако киберпакети за атака на противниците пътуват през далекосъобщителната мрежа на неутрална страна, то не би било допустимо да се атакува тази мрежа, за да се спре атаката, докато услугите се предлагат безпристрастно и за двете страни и неутралната страна само пренася пакетите без оглед на тяхното съдържание. Но ако противникът е проникнал в компютрите на неутрална страна и ги използва, за да започне своята атака, би било допустимо да се контраатакуват тези машини, ако неутралната страна отказва или не е в състояние да помогне.

По принцип, кибератаки срещу противник в рамките на хибридната война може да се считат за етични, ако следват горните принципи. В действителност, кибератаките са по-малко разрушителни, отколкото физическите атаки и по тази причина са предпочитани по хуманитарни причини. Вместо бомбардиране на изчислителен център, за да се спре определена услуга, като по този начин се причинят големи имуществени щети и евентуално загуба на живот, човек може да проникне или да наруши компютърните системи по начин, който изпълнява същите цели, но с по-малко щети и дългосрочни странични ефекти.

В заключение може да се обобщи, че оценяването на етичността на кибератаките като компоненти на хибридната война с традиционните форми на международното право е възможно, но не и при механично пренасяне на съответните норми. Спецификата на киберпространството и на действията в него изискват намиране на отговори на незадавани до момента въпроси, които касаят не само техническата страна, но също така нормативната и социалната сфера.

Използвана литература:

1. Diane Bailey. Cyber Ethics. The Rosen Publishing Group, 2008

2. Димов П., Ж. Желев. Хибридната война като част от общата теория на войната. https://postvai.com/analizi/хибридна-война.html

3. Георгиев Венелин. Човешкият фактор в киберсигурността. Авангард, 2016