БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ЗА ДЪРЖАВАТА И ПРАВОТО
СЕКЦИЯ ПО МЕЖДУНАРОДНОПРАВНИ НАУКИ

Елена Иванова Стоянова

МЕЖДУНАРОДНОПРАВНА УРЕДБА НА БОРБАТА С КИБЕРПРЕСТЪПЛЕНИЯТА

АВТОРЕФЕРАТ

на дисертационен труд за
присъждане на образователна и
научна степен
„доктор”

София, 2015

БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ЗА ДЪРЖАВАТА И ПРАВОТО
СЕКЦИЯ ПО МЕЖДУНАРОДНОПРАВНИ НАУКИ

Елена Иванова Стоянова

МЕЖДУНАРОДНОПРАВНА УРЕДБА НА БОРБАТА С КИБЕРПРЕСТЪПЛЕНИЯТА

А В Т О Р Е Ф Е Р А Т

на дисертационен труд за присъждане на образователна и научна степен „доктор”

Научна специалност

Международно право и международни отношения

Научен ръководител

Проф. д-р Ирена Илиева

София, 2015

Дисертационният труд е обсъден и насрочен за публична защита от секция „Международноправни науки“ на Института за държавата и правото при Българската академия на науките на 27 ноември 2015 г.

Дисертационният труд включва 228 страници. Състои се три глави, предговор, заключение, използвана литература.

Защитата на дисертационния труд ще се състои на 4 април 2016 г. пред научно жури в състав:

Вътрешни членове:	Проф. д-р Ирена Илиева
	Доц. д-р Маргарит Ганев
Резервен член:	Проф. д-р Жасмин Попова
Външни членове:	Проф. д.ю.н. Орлин Борисов
	Проф. д-р Габриела Белова
	Проф.д-р Надя Бояджиева
Резервен член:	Проф.д-р Пламен Пантев

Дисертационният труд и материалите по защитата са на разположение в Института за държавата и правото при Българската академия на науките (гр. София, ул. Сердика No 4) и на интернет страниците на Института и БАН.

П Р Е Д Г О В О Р

Един от фундаменталните проблеми на съвременното международно право и международни отношения е сигурността. Във века на информационните технологии, освен тяхното положително въздействие върху общественото развитие, се наблюдава и силно изразена негативна страна, а именно: киберпрестъпността.

Проблемите, свързани с киберпрестъпленията, и в частност тяхната международноправна уредба, не са били досега предмет на цялостно и задълбочено научно изследване в българската международноправна литература. Спецификата на представения труд се обуславя от интердисциплинарното естество на изследвания проблем. Успешното решаване на поставената научна задача изисква знания освен по международното публично право, също и от други научни области: информационни технологии и компютърни системи и мрежи, киберсигурност, право на Европейския съюз, вътрешно и международно наказателно право, и др.

Именно триединният характер на темата на дисертацията доказва безспорността на нейната актуалност. От това следва, че изходните методологически позиции при разработването на настоящия дисертационен труд са международното публично право и международното наказателно право.

На първо място, във века на информационните технологии, киберпрестъпленията са доказателство за реалността на „виртуалното правно пространство". От друга страна, от наказателноправен аспект, както отбелязва бившият главен прокурор на РБ Н. Филчев, „престъпността не е вечно и неизменно явление – тя се променя с хода на историята и се определя в крайна сметка от обществено-икономическите условия". Основите на международното наказателно право у нас са разработени от Д. Михайлов. Те са доразвити от бившия главен прокурор и настоящ председател на КС Б.

Велчев, който изследва и някои от киберпрестъпленията – напр. разпространение на порнография и др.

На второ място, според д.ю.н. О. Борисов международното публично право е главен регулатор на съвременната система на международните отношения в планетарен мащаб. Във френската правна доктрина международното право се определя като право, прилагано в международните отношения. Тази формула, с известни различия, днес е сред основните и най-семплите. Характерната през последните години глобализация на световната икономика и ускореното развитие на информационните технологии създава предпоставки за нови проявни форми на престъпната дейност, в частност киберпрестъпленията. В международноправната доктрина се отбелязва, че глобализацията на социално-икономическите процеси породи и глобализацзия на престъпността, която е все по-организирана и се превръща в транснационална. Престъпните организации много често реагират по-бързо от държавните системи на развитието на всички типове комуникации. Днес е назряла необходимостта от научен подход в борбата с престъпността, и в частност с особено усложнената и застрашаваща устоите на съвременното общество кибепрестъпност.

На трето, но не на последно място по значение, от международноправен аспект транснационалната киберпрестъпност изисква адекватен отговор и противодействие чрез съгласуваните действия на международната общност. Както е известно, принципът за сътрудничество между държавите е един от основните принципи на международното право, закрепен в Устава на ООН /норма jus cogens/. Необходимостта от сътрудничество между държавите в борбата с престъпността се обуславя от особения характер на киберпрестъпленията, засягащи понякога много държави, както и координация за предотвратяване на престъпните деяния, и не на последно място оказване на взаимопомощ при разследването на наказателни дела.

Предмет на изследване са киберпрестъпленията и тяхната международноправна уредба, и по-конкретно: нелегалният достъп до компютърни системи, разпространението на детска порнография в мрежата,

престъпленията срещу авторските и сродните им права, кражбата на лични данни, престъпленията срещу платежните инструменти и др. Киберпрестъпленията по своето естество надхвърлят националните граници и борбата срещу тях може да бъде ефективна единствено чрез международно сътрудничество. Това обуславя и необходимостта от изследването на този аспект и важната роля на съвместните усилия на международноправните субекти. С снование Ю. Бояджиева отбелязва, че борбата с тези престъпления придобива все по-голяма актуалност и поради използването на електронизирани системи и мрежи от местни и транснационални престъпни групировки и терористични организации. Терористичният акт в Париж на 13 ноември 2015 г. разкрива нов тип престъпност, и по-скоро преплитане на организираната престъпност с киберпрестъпността - по данни на германските медии оръжието, с което е извършено нападението, е закупено по интернет. Това поставя нови предизвикателства пред международноправната уредба на тези престъпления.

Правилният методологически подход изисква да се направи кратък исторически преглед на възникването и развитието на киберпространството – това е, от една страна средата, в която се извършват киберпрестъпленията, а от друга страна компютрите и компютърните системи са средство за осъществяването на тези престъпления.

В структурно отношение тези проблеми са разгледани в три глави, както следва: исторически преглед и разглеждане на понятието за киберпрестъпление, представяне на различните видове киберпрестъпления, анализ на европейската и международноправната уредба. Основният фокус е върху Конвенцията за престъпления в кибернетичното пространство, която в момента е основният действащ международноправен акт в тази област.

Методологическа основа на изследването са историческият метод, сравнителноправният метод, както и системният подход. Задълбочено се изследва възникването и развитието на киберпространството и появата на киберпрестъпленията в социално-икономическата среда. Сравнителноправният анализ включва задълбочен преглед на обширната и

некодифицирана международноправна и европейска правна уредба на киберпрестъпленията. Системният подход се изразява в анализ както на наказателноправната, така и на международноправната регламентация.

Всичко това обосновава както теоретичната новост на изследването, така и несъмнената практическа полза от него.

Глава I
История и развитие на Интернет и на престъпленията в киберпространството

Успешната борба с киберпрестъпленията изисква преди всичко да се разкрие средата, в която се осъществяват тези престъпления. Правилният методологически подход предполага кратък исторически преглед на възникването и развитието на интернет и на киберпрестъпленията.

Историята на Интернет и киберпространството започва като научна фантастика. За пръв път терминът „киберпространство" се появява в романа „Neuromancer" (1984 г.) на не толкова популярния американски писател Уилям Гибсън - около десет години по-късно се оказва, че версията на Гибсън е по-близко до реалността, отколкото някой е предполагал при издаването на романа.

В наши дни киберпространството неправилно се идентифицира с понятието за интернет. За да се направи необходимото разграничение в дисертационния труд се представя начинът, по който функционира киберпространството.

Понятието интернет се появява за пръв път през 1968 г. в документ, изготвен от Министерството на отбраната на Съединените щати, с който се създава Агенцията за сложни изследователски проекти (Defence Advanced Research Projects Agency, DAPRA).

Интернет пространството представлява лесно уязвима среда за криминални прояви главно поради две причини: дава възможност за анонимност и надхвърля географски граници. По този начин това става

предизвикателна среда за престъпния контингент, притежаващ съответните технически и езикови умения.

Историята на интернет престъпленията е почти толкова стара, колкото и самият интернет. Първата криминална проява в киберпространството датира от 40-те години на миналия век, почти от времето, когато е създаден първият компютър. През следващите години, с развитието на глобалната мрежа в условията на "световна икономическа цялостност", международните интернет престъпления се разрастват и започват да придобиват различни форми на проявление.

Кибератаките стават все по-чести и по-разрушителни през последните години – насочени са не само срещу правителствени учреждения, корпоративни и политически организации, а и срещу частни лица. Компютърните престъпления започват да стават доминиращи особено в развитите страни.

Прави се кратък обзор на развитието на киберпрестъпността в САЩ, Западна Европа, Австралия и др. В развитието на киберпрестъпността се наблюдават етапи на скокообразно нарастване в съответствие с навлизането на нови поколения електронна техника и нови комуникационни средства. През 2011 г. 556 милиона потребителя са станали жертва на киберпрестъпления в световен мащаб.

Според статистиката голям процент от извършените престъпления остават нерегистрирани - резултати от проучване на Станфордския изследователски институт в САЩ сочат, че още в началото на 90-те години 85% от електронните кражби остават неразкрити. Тревожни са и резултатите от проведено през 2002 г. проучване на Институт за компютърна сигурност в САЩ относно сигурността на информационните системи. Основна част - 90% от анкетираните компании са регистрирали пробиви в системите за сигурност, а 80% са претърпели финансови щети от проникванията в компютърните системи.

Латентността е иманентна характеристика на престъпността - по отношение на престъпността в киберпространството този въпрос стои в изключително

висока степен - размерът на скритата престъпност в компютърната среда е значително по-висок от традиционната престъпност.

Въз основа на историческия преглед на киберпространството и киберпрестъпленията се прави извод, че възможните щети и загуби варират от опасността за ограничен достъп до персоналния компютър до срив в системата на големи корпорации и институции, кражба на търговска конфиденциална информация, блокиране на правителствени сайтове и др. Финансовите загуби в резултат от киберизмама или саботаж могат да достигнат милиони долари или евро.

Глава II
Понятие и видове киберпрестъпления

В § 1 се разкрива понятието за киберпрестъпление (престъпление в кибернетичното пространство", "компютърно престъпление", "свързано с компютрите престъпление").

Въз основа на критичния анализ на множеството международноправни актове и документи, вкл. такива на ООН, ОИСР и др., на вътрешното наказателно законодателство на редица развити държави, вкл. българския НК, както и на международноправната доктрина, се прави извод, че понятието киберпрестъпление е всяко престъпление, което включва компютър или компютърна мрежа.

Конвенцията за престъпления в кибернетичното пространство /вж. по-долу/ и нашия НК използват понятията „компютърни данни" и компютърни системи" /чл. 93 НК/. Това придава на този вид деяния също и транснационален характер, от което следва, че компютърните престъпления имат както международноправен, така и наказателноправен аспект.

Липсата на легално определение позволява придаване на широко съдържание на това понятие в доктрината.

В дисертационния труд се поставя въпросът дали е допустимо разширително тълкуване на нормативната уредба на това понятие от гледна

точка на наказателното право. Известно е, че разширителното тълкуване не е допустимо и следва да се избягва в наказателноправната доктрина и практика.

В някои регионални международни актове, с цел ефективната борба с тероризма и морското пиратство, напр., е прието по принцип недопустимото в наказателното право разширително тълкуване.

Понятието за киберпрестъпление понастоящем се използва за широк спектър деяния, които обхващат както „традиционни" компютърни престъпления, така и престъпления, извършени в мрежата. Тези деяния са твърде разнообразни, за да бъдат успешно обхванати от строго и тясно определение. Неговото тълкуване е различно и според нормативните уредби на отделните държави.

Поради тази причина в дисертационния труд се предлага приемането на широко определение за киберпрестъпление, което да бъде приложимо спрямо потребностите на съответните държави, и също така да отговаря на бързото развитие на компютърните технологии.

В § 2 се разглеждат различните видове киберпрестъпления. В дисертацията е възприет следният подход: първо се представя кратка криминологична характеристика на престъпното деяние, след това се посочват релевантните правни разпоредби според Конвенцията за престъпленията в кибернетичното пространство, българското и чуждестранното наказателно законодателство. Критичен анализ на тези и на други международни актове се прави в следващата глава III на дисертационния труд.

Липсата на системни статистически изследвания не позволява да се очертаят не само размерите и тенденциите на престъпността в кибернетичното пространство, но и предметната й структура, т.е. видовете престъпления. Известна представа за тази структура дават някои отделни статистики и емпирични изследвания.

Опит за структуриране и подреждане на различните видове престъпления прави Ю. Бояджиева. Тя разделя компютърните престъпления на същински компютърни престъпления (престъпления против интелектуалната

собственост, престъпления против неприкосновеността и сигурността на компютърни системи и мрежи, и престъпления против неприкосновеността на компютърни данни) от една страна, и компютърно свързани престъпления от друга страна: престъпления против паричната, кредитната, финансовата и данъчната система, документни престъпления, престъпления против телекомуникациите, престъпления, свързани със съдържанието, престъпления против личността, престъпления против националната сигурност, мира и човечеството. Трудно е да се направи рязка граница между същинските и компютърно свързаните престъпления. В някои случаи т.нар. същински компютърни престъпления се припокриват с компютърно свързаните престъпления (напр. различните проявления на престъпленията против интелектуалната собственост), или пък различните деяния биха могли да бъдат причислени и към едната, и към другата група, според проявлението им, конкретно настъпилия резултат или начина на извършване. Такова разделение липсва в Конвенцията за престъпления в кибернетичното пространство. Тя разграничава четири основни групи престъпления, което води до някои припокривания в съответните категории. Конвенцията не обхваща всички проявления на престъпни деяния в киберпространството, но урежда основните им форми.

В този параграф, на основата на сравнителноправен анализ, се прави преглед и се разкриват основните характеристики на видовете комютърни престъпления:

1. **Престъпления срещу тайната, неприкосновеността и възможността за ползване на компютърни данни и системи:**
   1.1 Нерегламентиран достъп (хакерство);
   1.2 Възпрепятстване функционирането на компютърни системи;
   1.3 Въвеждане на вредоносни компютърни програми;
   1.4 Посегателство срещу неприкосновеността на данните / компютърен саботаж/;
   1.5 Незаконно прихващане на компютърни данни;

1.6 Шпионаж;

2. Компютърни престъпления:

2.1 Компютърна фалшификация;

2.2 Компютърна измама;

3. Престъпления, свързани със съдържанието:

3.1 Разпространение на порнографски материали (без детска порнография);

3.2 Детска порнография в интернет;

Детската порнография е изключително тревожен и широко дискутиран въпрос. Поради изключително важното значение на този въпрос се отделя специално внимание.

3.2.1 Проблеми, свързани с дефинициите

Някои държави възприемат много общи дефиниции на детска порнография, които съдържат субективен елемент, и се осланят на възможността за свободна преценка в наказателно-процесуалната система, чрез която да бъде постигнат необходимият резултат (в този контекст само като примери могат да се посочат Австралийският национален наказателен кодекс и Наказателният кодекс на Канада).

Постигането на международно споразумение за определението детска порнография е трудно поради гореизложените причини. Чл. 9 от Конвенцията за престъпленията в кибернетичното пространство дава отчасти отговори на някои от тези въпроси.

3.2.2 Съвременни прояви и разпространение на детската порнография

Прави се кратък преглед как се зараждат и разпространяват престъпленията срещу деца в цифрова среда.

3.2.3 Правна уредба и правни инициативи

Както бе посочено по-горе, престъпленията, свързани с детската порнография, са регламентирани в чл. 9 от Конвенцията за престъпленията в кибернетичното пространство. В дисертацията подробно са разгледани и анализирани нормативната уредба и правните инициативи относно престъпленията, свързани с детската порнография.

На това място следва да се отбележи, че резервата в чл. 9, т. 4 от Конвенцията позволява на всяка от страните да не инкриминира снабдяването или притежаването на детска порнография в компютърната система или на електронен носител. Производството, предлагането на възможност за достъп, както и разпространяването на детска порнография чрез компютърни системи следва да бъде инкриминирано от страните членки.

С оглед гарантиране и защита правата на децата в дисертационния труд се предлага de lege ferenda да се увеличат санкциите за извършени киберпрестъпления, свързани с детската порнография.

3.3 Проповядване и подбуждане към расова вражда, омраза и расова дискриминация;

3.4 Други престъпления, свързани със съдържанието;

Други престъпления, свързани със съдържанието, са напр.: незаконният хазарт и онлайн игри – уреден различно в отделните държави – напр. чл. 327 от българския НК; не са предвидени като престъпление във всяко национално законодателство и това дава възможност на извършителите да изберат мястото на действието.

3.5 Престъпления, свързани със съдържанието и свободата на изразяване;

4. Престъпления, свързани с авторското право и сродните му права/ компютърни престъпления против интелектуалната собственост

4.1 Същност на престъпленията

По своята същност, този вид деяния представляват посегателство срещу интелектуалната собственост.

Преглед на становищата за авторското право в българската правна доктрина прави д.ю.н. Цв. Каменова.

4.1.1 Софтуерно пиратство;

4.1.2 Пиратство на интелектуални продукт;

4.2 Правна уредба

4.2.1 Компютърните престъпления против интелектуалната собственост в Конвенцията за престъпления в кибернетичното пространство;

4.2.2 Компютърните престъпления против интелектуалната собственост в българското законодателство;

Анализът на правната уредба и доктрината в дисертационния труд дават основание да се предложи *de lege ferenda* увеличаване на санкциите за киберпрестъпления срещу авторското право.

5. Други видове киберпрестъпления

5.1 Кибертероризъм;

5.2 Кибервойна;

5.3 Престъпления в сферата на електронните платежни инструменти;

5.4 Кражба на самоличност;

5.5.Пране на пари и други престъпления против паричната и финансовата система;

Глава III

Нормативна уредба на престъпленията в кибернетичното пространство

В § 1 се разглежда развитие на нормативната уредба на престъпленията в кибернетичното пространство.

С основание в дисертационния труд се поставя въпросът: с какво киберпрестъпленията са по-различни и дали наистина са нов вид международни престъпления - някои от гореизброените деяния (измама, кражба, нелегална порнография и т.н.) са регламентирани в съществуващата нормативна уредба. Въпреки че повечето държави постоянно допълват и актуализират наказателните си закони, интернет средата създава предпоставки за появата и развитието на множество престъпни деяния с международен характер. Настоящите закони не са били създадени с идеята за такъв вид престъпления. Така например, оръжието за извършването на терористичните актове в Париж на 13 ноември 2015 г. е било закупено онлайн. Разследването би се затруднило изключително много, ако плащането е извършено с виртуалната валута биткойн. В тази връзка може да се предложи *de lege ferenda* да се криминализира покупко-продажбата на оръжие по интернет. Наблюдава се преплитане на тероризма с киберпрестъпленията.

Именно това превръща борбата с транснационалните киберпрестъпления в особено предизвикателство за правната уредба както в Европейския съюз, така и в международен аспект. В този параграф се прави преглед на инициативите, предприети в борбата с компютърните престъпления в рамките на ЕС и на международно ниво.

1. Инициативи на ЕС и на Съвета на Европа

В дисертацията се прави критичен анализ на няколко основни актове, част от които представляват съобщения на Европейската комисия.

1.2 Правна същност на Съобщението

За да се разкрие правилно и анализира обхвата на международноправната уредба на киберпрестъпленията е необходимо да се разкрие и правната същност на Съобщението. Прави се подробен преглед и задълбочен анализ на доктрината и практиката на СЕО (сега СЕС) по този въпрос.

Съобщенията на ЕК не са предвидени нормативно изрично сред източниците на правото на ЕС, нито в първичното, нито във вторичното право на ЕС. Въз основа на анализираните в дисертацията становища се прави извод, че в доктрината се предлагат различни варианти на класификация на тези актове - подкрепя се направеното предложение да се обособи група под наименованието „нетипични актове" /д.ю.н. А. Семов/.

Следващият принципен въпрос във връзка с правната същност на съобщението е този за неговото съотношението с вътрешните правни актове - това се налага поради липсата на европейска правна уредба относно съобщението.

В нашата правна доктрина се поставя въпросът: може ли министерският съвет да приема първични подзаконови нормативни актове? От една страна, в гражданскоправната литература се приема, че МС може да приема първични ПНА. От друга страна, в административноправната литература се поддържа обратното становище. Приема се, че издаването на ПНА, даващ първична уредба, означава превратно упражняване на предоставените от Конституцията прерогативи.

Логично е да се направи аналог между вътрешноправните и европейските актове. В дискусионен порядък се поставя въпросът: възможно ли е да се приема първична правна уредба с актове на ЕС от категорията на съобщението? Отговорът на този въпрос може да се търси при задаването на интересен паралел: ако се приеме аналог между закона и първичните източници на ЕС като първични актове; респ. ПНА и нетипичните актове на ЕС, сред които попада и съобщението, като вторични или производни. Както стана

ясно, във вътрешноправен аспект българската правна доктрина допуска първична правна уредба с ПНА на МС. Пренасяйки аргументите в полза на това твърдение на европейска плоскост, следва да се отговори, дали нетипичните актове, и по-специално дискутираното в този анализ съобщение, е акт на изпълнително-разпоредителна дейност и дали се издава въз основа и в изпълнение на други, първични актове на ЕС, или пък урежда неуредени досега обществени отношения и има за цел създаване на първични правни норми. За приемането на такава същност на съобщението, следвайки гореизложената логика и аргументи, е необходимо то да урежда материя, която преди това да не е била уредена изрично с първичен източник на ЕС, кореспондиращ на закон. Трудно е да се приеме такава значимост на нетипичните актове и в частност на съобщението. Както бе посочено, спорна е дори обвързващата правна сила на този акт.

От обоснованото становище на д.ю.н. А. Семов може да се заключи, че ако се приеме, че в едни случаи съобщението в зависимост от волята на автора има обвързваща сила спрямо адресатите му, а в други случаи няма обвързващо действие спрямо държавите, тогава логичният извод е: съобщението не е източник на правото на ЕС. Това е така, защото правото не познава такава категория актове, които в едни случаи да имат обвързваща сила, т.е. да бъдат евентуално от категорията на нормативните, а в други случаи да нямат обвързваща сила. Такава категория нормативни актове - източници на правото, не съществува.

Направеният анализ води до извода, че на плоскостта на правото на ЕС подобен аналог между съобщението и източниците на правото на ЕС трудно може да се постави и разисква. Тогава възниква въпросът, какъв акт е съобщението. Може да се направи извод, че то е от категорията на общите ненормативни актове. Ненормативен е, защото не съдържа абстрактни правила за поведение (правни норми). Няма такава правна норма, която веднъж да е задължителна, а веднъж не, а обвързващата сила на съобщението е под въпрос. Актът е общ, защото има неопределен кръг адресати, т.е., държавите-членки, за разлика от индивидуалните актове.

Направеният анализ и извод са необходими с оглед прегледът, който се прави в дисертационния труд на отделните съобщения, издадени от ЕК във връзка с борбата с киберпрестъпленията.

1.2.2 Съобщение COM (1996) 487 на Европейската комисия относно нелегалното и вредно съдържание в Интернет (Illegal and harmful content on the Internet/

В резултат на направения анализ на Съобщението се прави обобщение, че още през 1996 г. Комисията поставя правилно насоките на борбата с нелегалното съдържание в интернет. Посочена е важността на съвместната работа на държавите-членки, а също и в международен аспект, развива се идеята за обмяната на информация и се подтикват държавите-членки да поставят минимални стандарти на ниво местно законодателство и регулации. Набляга се на необходимостта от единна правна уредба относно отговорността на интернет-доставчиците и хостинг компаниите, както и тяхното саморегулиране и съвместна работа.

1.2.3 Съобщение COM (1999) 687 на Европейската комисия „Информационно общество за всички (An information society for all)

Анализът разкрива, че поставените цели се покриват със задачите на разгледаното по-горе Съобщение. Както планът, така и Съобщението съдържат важни стратегии за развитието на информационното общество, но не съдържат специфични наказателноправни предложения и правила, насочени към предизвикателствата, които поставя кибернетичната престъпност.

1.2.4 Съобщение на Европейската комисия COM (2000) 890 Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime – Създаване на по-сигурно информационно общество чрез подобряване на информационната сигурност и борба с компютърната престъпност

Ретроспективният преглед на актовете, приети от ЕК, води до заключението, че от момента на издаване на настоящото Съобщение досега се е развил, както спектърът на престъпните деяния, така и правните инструменти, насочени срещу тях. Съобщението посочва необходимостта от адекватни материалноправни и процесуалноправни инструменти на глобално, или поне на този етап на европейско ниво. От анализа на разгледаното Съобщение може да се направи също извод, че ЕК набляга еднакво както на законодателните, така и на всякакви извънзаконодателни инициативи в стремежа към изграждането на единна и сигурна информационна мрежа още в началото на новия 21-ви век. Разработването на превантивни инструменти, специализираните обучения, съвместната дейност на институциите на национално и международно ниво са точно толкова значими, колкото и законодателните предложения, които Комисията предвижда да предложи на европейско и международно ниво. Инициативите на Европейската комисия вече придобиха международно значение и своето завършено институционално измерение в създаването и развитието на центровете за борба с киберпрестъпленията.

1.2.5 Рамково Решение 2001/413/ПВР на Съвета от 28 май 2001 г. относно борбата с измамата и подправянето на платежни средства, различни от парите в брой

През 2001 г. Съветът на Европа публикува първото правно решение, което директно е насочено срещу киберпрестъпността. За разлика от съобщението, решението е правен акт на Съюза, посочен в чл. 288 ДФЕС (пред. чл. 249 ДЕО). Решението е акт, който има конкретен адресат.

1.2.6 Рамково Решение 2004/68/ПВР на Съвета от 22 декември 2003 г. относно борбата със сексуалната експлоатация на деца и детската порнография

1.2.7 Рамково Решение 2005/222/ПВР на Съвета от 24 февруари 2005 г. относно атаките срещу информационните системи

1.2.8 Рамкови решения относно борбата с тероризма

Първото такова решение е Рамково Решение на Съвета от 13 юни 2002 г. относно борбата срещу тероризма (2002/475/ПВР). То поставя някои въпроси, напр. дали приемането на това Решение от страна на Съвета не е прекомерна мярка, и дали е достатъчно аргументирано, особено от наказателноправна гледна точка. Според българското определение за умисъл в чл.11/2/ НК "Деянието е умишлено, когато деецът е съзнавал общественоопасния му характер, предвиждал е неговите общественоопасни последици и е искал или допускал настъпването на тези последици." Макар и да е предвидено в българския НК, с оглед на универсалния характер на това определение то би могло да бъде изходна точка за разсъждение. Както е известно, има два основни вида умисъл: пряк /директен/ и евентуален /косвен/, съобразно с това, дали деецът цели или само допуска настъпването на общественоопасните последици. При прекия умисъл са налице и интелектуалният, и волевият елемент. Умисълът е винаги конкретен, както е конкретно всяко престъпление. В разглеждания случай не може да се говори за пряк умисъл. Публикуването на материал, съдържащ инструктаж относно експлозиви или оръжия не съдържа непременно волята за терористичен акт. Възможно е крайната цел на разпространението на такъв вид материали въобще да не е терористичен акт или свързани с това действия, но е факт, че предвиждането, допускането и примиряването с настъпването на такива са елемент от умисъла на дееца.

1.2.9 Съобщение COM (2007) 267 на Европейската Комисия до Европейския парламент, Съвета и Европейския комитет на регионите „Към основна политика по отношение на борбата с престъпленията в кибернетичното пространство"

1.2.10 Препоръка No (95) 13 за проблемите на наказателнопроцесуалното право, свързани с информационните технологии

От направения анализ на изброените актове може да се направи изводът, че европейските институции и в частност ЕК са били особено активни в тази насока през последните десетилетия. Предприети са мерки в различните сфери на проявление на трансграничните престъпни деяния в киберпространството. Направен е сериозен опит да се реагира адекватно на бързопроменящата се киберсреда и появата на нови и нови престъпни деяния в нея. Все пак, въпреки широкия обхват и разнообразието на разгледаната материя в европейски мащаб, по-прецизен поглед показва, че киберпрестъпленията изискват по-задълбочена и изчерпателна правна уредба не само на европейско, но и на международно ниво.

Затова в § 2 се прави задълбочен анализ на най-значимия към настоящия момент международен акт за регулиране на киберпрестъпленията: **Конвенцията за престъпленията в кибернетичното пространство**. В дисертацията се прави кратък исторически обзор на преговорите, препоръките, подписването и целите на Конвенцията.

Специално внимание се отделя на въпроса, свързан с **определянето на юрисдикцията при киберпрестъпленията** - той е централен не само за Конвенцията, а представлява и принципен проблем в международното наказателно право. Не е достатъчно да се изясни и анализира нормативната уредба на киберпрестъпленията. Важно е на практика да се стигне до реализиране на съответната наказателна отговорност. За целта се изследва въпросът за приложимата юрисдикция – на основата на международноправната уредба, правната уредба в редица държави, както и конкретни примери от практиката.

Като типични трансгранични престъпления при киберпрестъпленията неминуемо се поставя въпросът: коя страна има правно основание да разследва деянието и да осъжда извършителите? Или, ако повече от една страна има юрисдикцията, как се определя чия юрисдикция ще има приоритет?

Подсъдността при киберпрестъпността далеч не е еднозначна. В повечето случаи страните нямат специфично законодателство и прилагат традиционните си правила за определяне на подсъдността. Често обаче

правилата са свързани със съответната територия, на която е извършено деянието, което при киберпрестъпленията е много относително. Някои държави, които имат специфични разпоредби за подсъдността при киберпрестъпленията (напр. Малайзия) стигат до разпоредби, според които могат да претендират за юрисдикция за деяние, извършено навсякъде по света. В Германия доминира доктрината за евентуално настъпване на увреждането, за да обоснове юрисдикцията си спрямо оператори на сървъри, разположени в Канада и действащи под канадско законодателство. Аргументът е, че сървърите нарушават германското антинацистко законодателство, т.к. могат да бъдат достъпни и от Германия. По тази логика може да се твърди, че доставчикът на интернет е субект на всички правни системи по света – привеждат се и конкретни примери от немската съдебна практика.

Други страни претендират за широко приложно поле на юрисдикцията с цел разследване на киберпрестъпления (напр. САЩ) - привежда се конкретен случай от практиката на ФБР.

Като алтернативно решение в доктрината се лансира идеята за създаването на отделен, независим режим на регулиране в киберпространството - това се предлага и възприема предимно от някои американски автори, според които на киберпространството може да се гледа като на „квази четвърто измерение", което може да подлежи на самостоятелно регулиране и представлява отделна, независима юрисдикция.

Това нетрадиционно предложение се отхвърля от преобладаващото мнение. Срещу този възглед се противопоставят преди всичко някои основни принципи на международното право. Всяка самостоятелна юрисдикция предполага суверенитет, а суверенитетът е неизменно свързан с държавността. Такава трудно може да бъде установена в киберпространството.

Алтернативните възгледи не дават отговор на противоречивите въпроси и казуси, поради това трябва да се търси решение въз основа на традиционните принципи за определяне на юрисдикцията в международното право.

В международното право сред основните принципи за юрисдикцията са териториалният, личният и универсалният.

Юрисдикцията по принцип обхваща три аспекта: определящ, т.е. властта да се определят приложимите норми в дадено общество; присъждащ, което очертава властта да се отсъди дали дадена норма е нарушена или не; и елементът на приложение и привеждане в сила, т.е. да се санкционира евентуалното неспазване на нормите, било то по съдебен, административен, или друг начин.

Повечето държави все още прилагат основно териториалния принцип и съответно националните си закони по отношение на киберпрестъпленията. Така обаче възникват редица трудности при определянето на locus delicti, а именно мястото, на което е извършено престъплението. Когато даден извършител извърши например неоторизиран достъп в система, има поне три възможни места, които могат да бъдат определени като locus delicti. От една страна, това би могло да бъде мястото, където физически се намира хакерът в момента на извършване на престъплението. От друга страна, релевантно е и мястото, където действат и където той прилага инструментите си за извършване на деянието. И не на последно място, еднакво важно е и мястото, където настъпва резултатът и където е локализирана целта и жертвата на деянието, и където де факто възниква резултатът от престъплението.

На този етап на европейско и международно равнище няма единодушие относно определянето на приложимата юрисдикция, респ. определянето на компетентния съд при извършването на киберпрестъпления. В правната доктрина се поставя въпросът: достатъчен ли е фактът, че даден уебсайт е достъпен от дадена държава, за база за юрисдикция на тази държава, или са необходими и други елементи, които да определят по-тясна връзка с въпросната държава. Първото решение крие риск от неограничена юрисдикция на всички държави, тъй като уебсайтовете почти винаги са достъпни отвсякъде. Това би означавало например, че при нарушаването на даден френски патент в мрежата, френски съд би могъл да упражни своята юрисдикция при определянето на спора, само защото въпросният сайт е

достъпен от Франция. При другата гледна точка се набляга на необходимостта от тясна връзка с държавата при посочване на приложимата юрисдикция. Това изискване би могло да доведе до определени ограничения, но всъщност отговаря напълно на правото на справедлив съдебен процес, чл. 6 от Европейската Конвенция за правата на човека. Основният елемент в подкрепа на това мнение е, че по този начин се избягва една универсална юрисдикция и неяснота при определянето й.

Универсално решение на тези проблеми не би могло да се търси на национално равнище. Необходимо е създаване на общи правила, приложими във всички държави в тази област. Това съответно би означавало създаване на специален режим, валиден само за киберпрестъпленията, който обаче не би бил приложим и за други деяния. На този етап липсва адекватно решение и на международно равнище. Основният международен акт - Конвенцията за киберпрестъпленията - не дава ясни критерии за определяне на locus delicti. Прави се задълбочен анализ на релевантните разпоредби на Конвенцията. Конвенцията оставя страните-членки да определят подсъдността на дадено престъпление, като ги задължава да вземат необходимите мерки за определяне на подсъдността, разбира се в рамките на основните принципи на международното право. В случай на конкуриращи се юрисдикции Конвенцията оставя на страните да определят коя от заинтересованите страни е в най-добра позиция да извърши съдебното преследване (чл. 22, ал. 5). В тази връзка важно е да се отбележи, че в такива случаи от решаващо значение е да се прилага принципът ne bis in idem с цел избягване на юридически конфликти.

По-специално се обръща внимание на чл. 22, ал.1, б. „г" от Конвенцията, регламентиращ личният принцип. Тази разпоредба съдържа две ограничения. Първото е, че страните по Конвенцията трябва да установят юрисдикция, когато престъплението е извършено от неин гражданин на територията на друга страна-членка, в случай, че престъплението е наказуемо там, където е извършено. Този механизъм е известен като т.нар. национален принцип. Второто ограничение е, че страните по Конвенцията трябва да установят

юрисдикция и когато извършеното престъпление не спада към териториалната компетентност на нито една страна по Конвенцията. Това ограничение очевидно се базира на по-широкообхватния универсален принцип (без той изрично да се споменава в Конвенцията). Приложимостта и валидността на този принцип не е еднозначна. Признато е, че универсална юрисдикция би могла да бъде приложима дотолкова, доколкото международното публично право упълномощава страните да я прилагат. Международни споразумения позволяват използването на универсалния принцип само при много тежки престъпления и при строги ограничителни режими с цел избягване на произволното му прилагане.

На последно място, но не и по-важност, се анализира чл. 22, ал. 2 от Конвенцията, според който всяка страна-членка може да направи резерва и да не прилага предвидените в чл. 22, ал. 1, букви „б, в, г" правила за определяне на подсъдността. Изключение прави териториалният принцип, уреден в чл. 22, ал. 1, б. „а", при който резервата не е приложима. Причината за резервата е, че на практика трудно би могло да се очаква, че изброените правни принципи-универсален, личен, трудно биха били приложими в рамките на всяко национално законодателство и да бъде съобразено с местните норми и традиции на всяка страна-членка.

Въз основа на направения анализ в дисертацията се прави извод, че определянето на приложимата юрисдикция при киберпрестъпленията е предизвикателство за международното наказателно право. Постигането на универсално решение на този етап е трудно постижимо, особено с оглед на бързоразвиващите се технологии. Създаването на общ режим рискува да не устои на бързото развитие на този тип деяния, а постоянното му актуализиране на този етап е непосилна задача за всяка юрисдикция, както и за международната правна рамка. Налага се прилагането на различен подход за всеки казус, което предполага гъвкави правни инструменти и готовност на всяка юрисдикция да тълкува правилно съответното наказателноправно законодателство. Развитието на международната уредба в тази област тепърва предстои, което заслужава интерес от страна на правната доктрина.

Международното сътрудничество според Конвенцията за престъпленията в кибернетичното пространство

Конвенцията разглежда три общи принципа на международното сътрудничество: свързани със сътрудничеството (чл. 23), екстрадицията (чл. 24) и взаимната помощ (чл. 25 и 26). В дисертационния труд се разглеждат основните проблеми в тази област. Предмет на анализ са и специалните разпоредби на Конвенцията в областта на международното сътрудничество при киберпрестъпленията, напр. ползването от дадена държава на доказателства от друга държава-членка, прилагането на процесуалните инструменти и др.

За да се даде ефикасен отговор на предизвикателствата на информационната епоха се оказва необходимо да се допълнят и формите на сътрудничество и взаимопомощ и между полицейските органи. Чл. 35 от Конвенцията въвежда едно средство, което се основава на опита, придобит в експлоатацията на една вече съществуваща мрежа, а именно - уникалното нововъведение на Г-8 за укрепване на международното сътрудничество: създаването на мрежа от специалисти по високи технологии, работеща 24 часа на ден, седем дни в седмицата, която представлява допълнителен международен канал за бързото получаване на технически и правни съвети и помощ. През 1997 г. Г-8 създаде мрежата 24/7 между своите държави-членки. Създаването на това звено от експерти, особено на такова, което работи в тясна координация с мрежата на Г-8, може да се окаже един от най-важните и трайни приноси на Конвенцията.

Разпоредбите на Конвенцията, посветени на международното сътрудничество, поставят напълно нова основа в международното право в момент, в който международната общност силно се нуждае от това. Те изпреварват далеч досега съществуващите конвенции по отношение на редица ситуации, за които се предвиждат разпоредби за нови средства за сътрудничество- средства, които все още не са били разглеждани. С това се увеличават възможностите на държавите да предприемат бързи и ефективни

действия в борбата с терористичната дейност чрез компютърните мрежи, а също така и по отношение на други международни кибернетични проблеми. Разпоредбите на Конвенцията по отношение на международното сътрудничество запазват съществуващите рамки за сътрудничество, като наред с това предвиждат и съществени гаранции за защитата на правата на човека и на други значими интереси. Тези разпоредби в крайна сметка формират солидна основа за бъдещи усилия за допълнително укрепване на общата рамка за сътрудничество.

Предмет на критичен анализ са и процесуалните разпоредби на Конвенцията. Уникалният характер на международните киберпрестъпления предполага и по-особени процедурни правила извън рамките на традиционното разследване. Обикновеното събиране и съхраняване на данни невинаги се оказва достатъчно ефективен метод при специфични кибератаки. Често разследващите органи са изправени пред предизвикателствата да съчетават традиционните методи с иновативни процедури.

Бързото запазване на данни в трафика е особено наложително за успешното разследване на киберпрестъпленията /чл. 16 от Конвенцията/.

Предмет на анализ е и чл. 18 от Конвенцията, който предвижда задължение за предоставяне на данни и информация на разследващите органи, като се прави разграничение на термина „компютърни данни" /чл. 18, ал. 1 а/ от „данни за абоната" /чл. 18, ал. 1 б/.

Претърсването и изземването на съхраняваните компютърни данни /чл. 19 от Конвенцията/ остават един от най-важните инструменти в разследването. Този инструмент става приложим след като органите са успели да идентифицират извършителя и следва да анализират съдържанието на компютъра и да изберат необходимите доказателства. Повечето страни-членки по Конвенцията имат такива норми в националната законодателна уредба. Все пак, съществуват някои специфики относно киберпрестъпленията.

Анализът на чл. 20 от Конвенцията /събиране на данни в реално време/, разкрива една от основните трудности в тази връзка - използването на анонимна комуникация от извършителите, било то чрез специални софтуери

или чрез обществени интернет терминали. В такива случаи идентифицирането на извършителя в повечето случаи е силно затруднено или остава невъзможно.

Съставът на чл. 21 от Конвенцията /прихващане на данни, свързани със съдържанието/, е сходен с този на чл. 20, но чл. 21 се отнася до данни, свързани със съдържанието. Тази норма е релевантна в случаите, в които разследващите са установили извършителя, но предстои да се анализира каква информация е обменена.

Едно от основните предизвикателства за разследването при чл. 21 от Конвенцията е използването на криптирана технология. Криптираната технология дава възможност на извършителя да защити съдържанието така, че разследващите органи нямат достъп до него. Така анализирането на съдържанието става невъзможно. Декриптирането в повечето случаи е трудоемко и често невъзможно.

Един от основните проблеми при гореизброените процесуални мерки е **конфликтът със защитата на лични данни**. Разследването на киберпрестъпността изисква специфични методи, които често поставят неприкосновеността на личните данни под въпрос. Открит остава и въпросът, редно ли е всички потребители да бъдат третирани като потенциални извършители на престъпления, и поради това личните им данни да бъдат следени и запазвани. Какво се случва тогава с адвокатската тайна например, когато адвокат телефонира или изпраща електронни съобщения с цел подготовка на защита на клиента си?

Направеният в дисертационния труд критичен анализ на международноправната уредба на киберпрестъпленията, на правната доктрина /американска, предимно немска и др./, както и на съдебната практика дават основание да се предложи *de lege ferenda* да се извърши кодификация на обширната и понякога противоречива нормативна уредба, свързана с киберпрестъпленията и разследването срещу тях, както и с оглед с оглед гарантиране правата на гражданите. С предлаганата кодификация ще се повиши равнището на нормативната уредба (напр. регламент или директива

на ЕС), ще се преодолеят някои противоречия на законодателство на ЕС с други международни актове, напр. Европейската конвенция за правата на човека, и др.

В § 3 предмет на анализ са инициативите на международно равнище:

1. Актове на ООН;

2. Актове на Международната асоциация по наказателно право;

3. Актове на Г- 8.

З А К Л Ю Ч Е Н И Е

Предмет на изследване в настоящия дисертационен труд е международноправната уредба на киберпрестъпленията. Систематизирани са всички видове компютърни престъпления и е направен критичен анализ на международноправната и националноправната уредба на този вид престъпни деяния.

За първи път в българската правна доктрина научно изследване се поставя на триединна основа: киберпространството, международно публично право и международно наказателно право.

Бързото развитие и усложняване на компютърните технологии увеличава страха от превръщане на мрежата в своеобразен „рай" за компютърните престъпления, поради това, че тя не попада под действието на никой от националните закони. Това предполага, че единствен адекватен отговор може да бъде представен на международно ниво.

В правната доктрина се приема, че международното наказателно право е нов правен отрасъл, който се формира през последните десетилетия на основата на международното публично право и наказателното право.

Задълбочено са разработени проблемите, свързани с компютърната фалшификация и измама, престъпленията срещу тайната и неприкосновеността на компютърни данни и системи, престъпленията, свързани със съдържанието, с авторското право и сродните му права, престъпления против интелектуалната собственост, детската порнография в интернет, кибервойната и кибертероризма, деянията в сферата на електронните платежни инструменти, прането на пари и др. Това са проблеми от изключително важно значение за всяка една държава и за международната общност като цяло. Борбата с престъпността се отнася към сферата на вътрешното законодателство на всяка държава. Същевременно, глобализацията на икономическите и социалните процеси поражда глобализация и на престъпността. Тя става все по-организирана и трансгранична.

Киберпрестъпленията са предмет на уредба както в националните законодателства, така и на международно ниво. В дисертационния труд се прави критичен анализ на нормативната уредба на киберпрестъпленията както на международноправната уредба, така и на българския НК.

Важно е да се отбележи, че това са проблеми не само на правната уредба, но също така и на правоприлагането, на разграничаването на юрисдикцията на отделните държави при транснационалните киберпрестъпления. Въз основа на направения анализ се прави изводът, че определянето на приложимата юрисдикция при киберпрестъпленията е предизвикателство за международното наказателно право. Постигането на универсално решение на този етап е трудно осъществимо, особено с оглед на бързоразвиващите се технологии. Създаването на общ режим рискува да не устои на динамиката на този вид деяния, а постоянното му актуализиране на този етап е непосилна задача за всяка юрисдикция, както и за международноправната уредба. Налага се прилагането на различен подход за всеки казус, което предполага гъвкави правни инструменти и висока степен на професионална квалификация на правоохранителните и правоприлагащите органи да тълкуват и прилагат прецизно съответното наказателноправно законодателство. Развитието на международната уредба в тази област тепърва предстои, което обуславя интереса на правната доктрина.

Основната международноправна уредба се съдържа в Конвенцията за престъпленията в кибернетичното пространство. Наред с нея са приети множество актове на ниво ЕС и други международни актове. В тази връзка се прави предложение *de lege ferenda* за кодификация на нормативната уредба на ниво ЕС- става въпрос за уредбата на политиката на киберсигурност в ЕС. Предимствата на кодификацията са безспорни. Тя е особено необходима в наказателноправната материя. Последният пример на преплитане на тероризма с киберпрестъпността /атентатът в Париж на 13 ноември 2015 г./ засилва необходимостта от усъвършенстване на международноправната уредба на киберпрестъпленията, вкл. криминализиране на покупко-продажбата на оръжие по интернет. На необходимостта от засилване на контрола върху

продажбата на оръжие обръща специално внимание и президентът на САЩ Б. Обама /особено след терористичния акт в Сан Бернардино през декември 2015 г./.

Проблемите на нормативната уредба на киберпрестъпленията са много и сложни. Настоящият дисертационен труд не претендира за тяхното изчерпателно изследване. Целта на автора е да обърне внимание на научната общност, на нормотворческите органи на ЕС и на националния законодател върху някои от тях. Универсално решение на тези проблеми не би могло да се търси на национално равнище. Необходимо е създаване на нормативна уредба в тази област, приложима във всички държави-членки. Това съответно би означавало създаване на специален режим, валиден за киберпрестъпленията. За успешното противодействие на киберпрестъпността е необходимо да се провеждат комплексни мероприятия с цел отстраняване на причините и условията, способстващи за извършването на тези деяния. Основен принцип на наказателното право е неотвратимостта на наказанието. Необходимо е държавите и международната общност да изпратят сигнал до престъпния контингент, че владеят положението. Това може да стане не толкова чрез тежестта на наказанията за извършени престъпни деяния, колкото чрез неотвратимостта на наказателната отговорност. Не може да има ефективна борба срещу кибепрестъпността без качествена международноправна наказателна уредба.

Направените предложения *de lege ferenda* засилват практическата насоченост на дисертационния труд.

НАУЧНИ ПРИНОСИ

Научните приноси се разкриват в две насоки: приноси с теоретична насоченост и приноси с практическа насоченост.

1. Приноси с теоретична насоченост:

1.1. Научното изследване в дисертационния труд е поставено на триединна основа:

- киберпространството като среда, в която се извършват киберпрестъпленията;

- международното публично право;

- международното наказателно право.

Този научен подход се прилага за първи път в българската правна доктрина.

1.2. За първи път в българската правна литература се изследва възникването и развитието на интернет като среда и като средство за извършване на киберпрестъпления.

1.3. За първи път в българската правна литература се прави цялостно и задълбочено изследване на международноправната уредба на киберпрестъпленията и борбата срещу тях. Изследвана е също и регионалната международноправна уредба на този въпрос.

1.4. Прави се задълбочен сравнително-правен анализ на международноправната уредба на киберпрестъпленията с вътрешната наказателноправна уредба на редица водещи западни държави /Германия, Великобритания, Холандия и др./, както и с българския НК.

1.5. За първи път в българската правна доктрина се прави анализ и се разкрива правната същност на Съобщението на ЕК на основата на сравнителноправния анализ с вътрешното законодателство на РБ.

1.6. Изследват се всички основни видове киберпрестъпления, разкриват се техните характеристики като транснационални престъпления и се определя понятието „киберпрестъпление”.

1.7. За първи път в българската правна литература се прави критичен анализ на практиката не само на СЕО, сега СЕС, но и на върховните съдилища на редица развити държави, напр. Германия, Холандия и др. относно киберпрестъпленията.

2.Приноси с практическа насоченост:

2.1. Предложения *de lege ferenda*:

2.1.1. Важно практическо значение за повишаване ефективността на борбата срещу кибепрестъпленията има предложението за кодификация на международноправната уредба на тези престъпления. Кодификацията на ниво ЕС е въпрос на уредбата на политиката на киберсигурност в ЕС.

2.1.2. Криминализиране на покупко-продажбата на оръжие по интернет. Този проблем става изключително актуален по две причини: а/след атентатът в Париж на 13 ноември 2015 г. се проявява тенденция на преплитане на тероризъм с киберпрестъпление; б/при евентуално реализиране на подобни сделки чрез bitcoin разследването на киберпрестъпленията би се усложнило и затруднило изключително много.

2.1.3. Увеличаване на санкциите за извършени киберпрестъпления, свързани с детската порнография и срещу авторското право в българския НК.

2.1.4. Да се предвидят в Конвенцията увеличени санкции за доставчиците на интернет-услуги при възпрепятстване на разследващите органи при извършени киберпрестъпления, както и в българския НК.

2.2. С практическа насоченост е изследването на международното сътрудничество според Конвенцията за престъпленията в кибернетичното пространство, особено при събирането на доказателства от разследващите органи.

2.3. Разкриването на характеристиките на киберпрестъпленията, вкл. анализът на съдебната практика, могат да бъдат полезни на разследващите и правораздавателните органи в борбата срещу тези престъпления.

2.4. Изследването относно определянето на компетентната юрисдикция при наказването на извършителите на киберпрестъпления е предизвикателство за международното наказателно право.

2.5. Изследването на необходимостта от гарантиране и спазване на правата на гражданите при разследване на киберпрестъпления и особено тайната на кореспонденция между адвоката и неговия клиент имат изключително голямо практическо значение.

СПИСЪК НА ОТПЕЧАТАНИТЕ НАУЧНИ ТРУДОВЕ

1. Анализ на Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство, Научни трудове на Института за държавата и правото, том VI, БАН ИДП, София, 2011 г., с.43-51

2. Кратък анализ на търговското споразумение за борба с фалшифицирането (АСТА), Научни трудове на Института за държавата и правото, том VII, БАН ИДП, София, 2012 г., с.253-262

3. Понятие и история на престъпленията в кибернетичното пространство, Правна мисъл, 1/2014, БАН ИДП, София, 2014 г., с. 55-63