ПРОТИВОДЕЙСТВИЕ СРЕЩУ КИБЕРПРЕСТЪПНОСТТА НА ГЛОБАЛНО И РЕГИОНАЛНО РАВНИЩЕ НА СИГУРНОСТ

доц. д-р Венелин Георгиев
Нов български университет

Дефиниране на понятията „киберпрестъпление" и „киберпрестъпност"

Голяма част от изследванията и публикациите в областта на киберпрестъпността започват с опити за дефиниране на този социален феномен. В резултат на тези опити се появяват множество различни определения за това добило в последно време висока популярност понятие. Според едни автори киберпрестъпността са отъждествява с всяко действие (деяние), при което като инструмент, цели или място на извършване се явяват компютърните системи или мрежи. Като пример за търсене на международно признато определение за киберпрестъпността може да се посочи Международната конвенция за подобряване на защитата срещу киберпрестъпността и тероризма, в която киберпрестъпността се определя като неправомерни действия срещу компютърните системи и мрежите в киберпространството.

При опита да бъдат конкретизирани и детайлизирани определенията за киберпрестъпността се достига до определение, според което същата се асоциира с действия, извършвани с помощта на компютърни системи, които могат да бъдат незаконни или неправомерни според нормативната уредба на една или повече страни и които могат да бъдат извършени с помощта на глобалните компютърни мрежи.

С прецизиране на определенията за киберпрестъпността се изпускат случаите, когато физическа информационна инфраструктура се използва за извършване на обичайни престъпления, но в същото време се рискува да бъдат изпуснати и случаите на престъпления, възприемани в международните норми като киберпрестъпления. Като пример, човек, който създава USB-устройство, съдържащо вредоносен софтуер, способен да унищожи информацията в компютърна система при включване на въпросното устройство към тази система, извършва престъпление. Друг пример, при тясното разбиране за киберпрестъпността едно копиране на данни с помощта на физическо устройство се приема за злонамерено, когато не се извършва в рамките на глобална компютърна мрежа. В случай че копирането на данни става в рамките на глобалните компютърни мрежи, същото не може да бъде класифицирано като киберпрестъпление. Дадените примери дават основание да се каже, че дефинирането на понятието киберпрестъпност среща значими трудности.

В практиката терминът киберпрестъпност се използва за определяне на широк спектър от правонарушения, включително традиционните компютърни правонарушения, а също така и мрежовите престъпления. Отсъствието на общоприето определение за киберпрестъпност не е от голямо значение до момента, в който киберпрестъпността се използва като юридически термин.

Както вече беше отбелязано, терминът киберпрестъпност не може да бъде асоцииран с или отнесен към едно общо и единствено определение. Той изразява или представя не толкова единичен престъпен акт, а по-скоро съвкупност или сбор от незаконни действия и поведения в киберпространството. Основното съдържание на термина може да бъде описано с помощта на макар и неизчерпателен списък от действия и поведения, които изграждат киберпрестъпността.

Различни автори, занимаващи се с проблемите на киберпрестъпността, се опитват да дадат дефиниция за понятието. В същото време в националното законодателство на отделните държави не може да се срещне единно прието определение. Интересни факти в това направление представляват следните[1]:

- при изследване на законодателството в областта на киберпрестъпността при повече от двеста страни едва при 5% се среща използване на термина киберпрестъпност в заглавията и съдържанието на специализираните закони;
- по-често срещани са термини като компютърна престъпност или престъпност на високите технологии;
- в голяма част от свързаните закони се разглеждат престъпления, включени в концепцията за киберпрестъпността, каквито са неправомерният достъп до компютърни системи и мрежи, кражба на данни и информация, измами с помощта на компютърни системи и др.;
- в случаите, когато терминът киберпрестъпност се използва в заглавие или съдържание на даден закон, обикновено в този закон не се дава ясна и точна дефиниция за киберпрестъпността;
- в случаите, когато терминът киберпрестъпност се включва в юридически определения, общият подход за дефиниране на термина е чрез изброяване на престъпленията, които са включени в съответния закон.

По подобен начин една много малка част от международните и регионалните законови инструменти се опитват да дадат определение за киберпрестъпността. Като примери могат да бъдат дадени:

- киберпрестъпността включва нарушения (престъпления) по отношение на сигурността на информацията;
- престъпленията срещу компютърната информация се изразяват в използване на информационни ресурси или на влиянието от тях (чрез тях) за незаконни цели.

Удобен подход при дефиниране на киберпрестъпността е изброяването на съвкупност от действия и поведения, които определят нейния обхват. Този подход е полезен с това, че поставя фокуса върху описанието на криминалното поведение в киберпространството. Подобен подход се използва при дефиниране на понятието корупция, при който се прави описание на действията, определяни като корупционни. Като обобщение може да се каже, че киберпрестъпността представлява съвкупност или система от специфични действия и поведение в киберпространството, противоречащи на установените правила.

При опита да бъде дефинирана киберпрестъпността с помощта на нейните ключови характеристики могат да се използват различни подходи. Един от тях фокусира вниманието върху обекта на престъплението, който може да бъде отделно лице, група лица, човешки ценности и т.н. Друг подход обръща внимание на факта, че при извършване на киберпрестъпление се били използвани компютърни системи и мрежи, както и услуги, които те предлагат. И при двата подхода не се изчерпват случаите на киберпрестъпления, но те дават добра основа за класифициране на престъпните актове. В таблица 1[2] е представена примерна класификация на действия, които изразяват същността на киберпрестъпността и които са разделени в три основни категории.

---

[1] Marko Gercke. Understanding Cybercrime: Phenomena, Challenges and Legal Response, 2012.

[2] Георгиев В. Противодействие срещу киберпрестъпността. София, Авангард, 2014.

Таблица 1. *Категории действия, определяни като киберпрестъпления*

1. Действия срещу конфиденциалността, интегритета и достъпността до компютърните системи и данни
- незаконен достъп до компютърни системи и мрежи
- незаконен достъп, придобиване или унищожаване на компютърни данни
- незаконна намеса във функционирането на компютърни системи и мрежи
- създаване, разпространение и притежаване на незаконни средства за неправилно използване на компютърни системи
- нарушаване на защитните мерки на компютърни системи
2. Действия по отношение на компютърни системи и мрежи, насочени към извличане на персонални или финансови ползи или нанасяне на щети
- измама и фалшифициране с помощта на компютърни системи
- престъпления с помощта на компютърни системи спрямо идентичността
- престъпления с помощта на компютърни системи спрямо авторските и търговските права
- изпращане или контролиране на изпращането на спам
3. Действие, свързани със съдържанието на данните и информацията
- създаване и разпространение на информация за пропагандиране на ненавист и омраза
- създаване, разпространение и притежаване на материали, съдържащи детска порнография
- създаване и разпространение на информация за поддържане и пропагандиране на тероризъм

Списъкът на действията в таблица 1 не е изчерпателен и към него могат да бъдат добавени следните действия:

- създаване и разпространение на компютърни средства за подпомагане на незаконни действия, свързани с финансови инструменти и средства за плащане;
- on-line хазартни игри;
- използване на компютърни средства за облекчаване на процесите за трафик на хора, наркотици и оръжия;
- нерегламентиран достъп до класифицирана информация и т.н.

При опита да бъде класифицирана с цел изучаване киберпрестъпността може да бъде разделена на такава, която е ориентирана към нанасяне на увреждания на информационните ресурси и информационната инфраструктура, и на такава, която е ориентирана към извличане на конкретни ползи за извършителите. Първият тип киберпрестъпност обикновено е дело на недоволни, неоценени и отстранени служители на организацията и се извършват вътре в рамката на самата организация. Вторият тип киберпрестъпления се извършват от престъпници, който са външни за организацията.

Компютърната престъпност може да бъде дефинирана също така и като всяко нарушение на закона, за чието разкриване, разследване и съдебно преследване се изискват познания в областта на компютърните технологии. В този смисъл като примери за компютърни престъпления могат да бъдат дадени саботажът, софтуерното пиратство, кражбата на лични данни и др.

Компютърната престъпност се олицетворява с престъпления, при които се използва компютърна система или мрежа и когато компютърът играе определена роля при извършване на самото престъпление. В този смисъл интернет престъпността се изразява в престъпно използване на интернет функциите и услугите.

При киберпрестъпността, ориентирана към извличане на ползи, престъпността се поддържа и улеснява от компютърни средства и мрежи, при което първичната цел не е самият компютър или мрежа, а тяхната защитеност и съдържащата се в тях информация.

От своя страна киберпрестъплението представлява термин, с който се определят атаки срещу киберсигурността, преследващи няколко цели. Първата цел се изразява в придобиване на нерегламентиран достъп до чувствителна информация на набелязаната цел. Голяма част от хората и организациите са зависими в значителна степен от запазване на конфиденциалността на информацията, с която разполагат, като пример: лични данни, информация за нови продукти, ценови листи, данни за търговски оборот и т.н. Извършителите на подобен тип атаки са в състояние да извличат директни ползи от придобитата информация или индиректни ползи за сметка на предоставяне (продаване) на информацията на заинтересовани лица. След получаване на нерегламентиран достъп до компютърната система на целта авторите на атаките също така могат да променят съдържанието или да унищожат чувствителна информация, което също се превръща в загуба за нейния притежател.

Като киберпрестъпление се определя всяко престъпление, което е предприето и реализирано по отношение на компютърна мрежа. В тези случаи киберпрестъплението не се ограничава единствено до атаки на мрежата отвън. Най-често срещаният тип киберпрестъпници се появяват и проявяват в рамките на самата организация и сред потребителите на мрежата. Съществува необяснимата практика една част от тези престъпления да се приемат като невинни и незначителни.

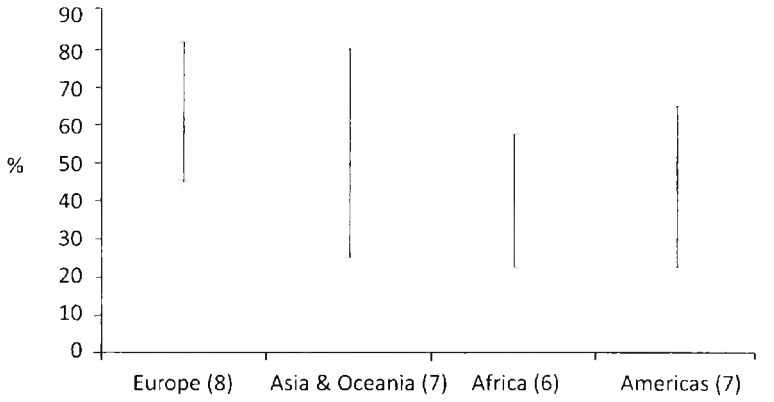
Киберпрестъпленията и компютърните престъпления са свързани с интернет престъпленията. Някои автори определят интернет като „нож с две остриета", който осигурява и предоставя различни възможности за развитие на отделните личности и на организациите. В същото време появата на интернет доведе до създаване на нови възможности за извършване на престъпления. Всеобщо споделяно мнение е, че интернет престъпленията са се превърнали в глобален проблем, противодействието срещу който изисква коопериране и участие както на развитите страни, така и на развиващите се страни на регионално и глобално равнище на сигурността.

Международен характер на киберпрестъпността

Киберпрестъпността далеч не е първата форма на престъпност, изискваща глобално противодействие. В историята на човечеството глобални по своя мащаб акции са прилагани срещу търговията с наркотици, трафика на хора и оръжие, международната организирана престъпност и т.н. От друга страна, безспорен е фактът, че киберпрестъпността днес поставя уникални предизвикателства пред международното сътрудничество по пътя на противодействието срещу нея. На фигура 1 е показан процентът на киберпрестъпленията, определени като носители на характеристики на международни престъпления.[3] Очевидно делът на киберпрестъпленията с международен характер (по региони съответно: Европа – 75%, Азия и Океания – 50%, Африка – 40%, Северна и Южна Америка – 30%) е достатъчен аргумент да бъде обърнато внимание на предизвикателствата и трудностите при противодействие на този вид специфична престъпност.

---

[3] Marko Gercke. Understanding Cybercrime: Phenomena, Challenges and Legal Response, 2012.



Фиг. 1. Дял на киберпрестъпленията с международен характер

Практиката показва, че днес повечето от жертвите на киберпрестъпленията са извън националните граници на извършителите (престъпниците). Използването на прокси сървъри и нарастващото влияние на социалните медии са сред факторите за растеж на броя на киберпрестъпленията с международен характер. Извършителите са напълно наясно със закононарушението и поради това използват интернет ресурси, като например електронна поща извън страната в опит да заличат свидетелствата за тяхното престъпление.

Редица автори в рамките на свои изследвания определят кои са основните характеристики, които дават основание дадено деяние в киберпространството да бъде определяно като престъпление с глобален или регионален мащаб. Резултатите от обобщението на тези изследвания показват, че:

- киберпрестъпленията се определят като престъпления с международен мащаб, когато част или всички деяния са извършени на територията на друга държава или когато извършителите (или част от тях) се намират на територията на друга държава;
- киберпрестъплението се определя като международно, когато е извършено на територията на повече от една държави;
- киберпрестъплението има характеристиките на международно престъпление, когато е извършено в една държава, но същото е подготвено, планирано и управлявано от територията на друга държава;
- глобалният характер на едно киберпрестъпление се определя от това, дали е извършено в една държава, но е подготвено от организирана група, действаща в повече от една държави;
- киберпрестъплението е с глобален характер и когато е извършено в една държава, но е нанесло значителни вреди на друга/и държава/и.

Изброените по-горе характеристики представляват само основни постановки, но съществуват и други подходи за определяне на международния характер на киберпрестъплението. Един от методите за характеризиране на всяко престъпление е да се определят елементите „извършване / поведение / провеждане", „обстоятелство" и „резултат". Там, където един от тези елементи се локализира или произведе съществени щети на друга територия, ще е наличен международен характер на съответното киберпрестъпление.

Международният характер на киберпрестъплението е наличен и когато *modus operandi* на нарушението попада в друга юрисдикция. Само извънтериториалните сървъри за компютърните данни, свързани с нарушението, може да не са достатъчни, за да се активира юрисдикцията на страната, където е сървърът, но е от съществена важност при събирането на доказателства и при процеса на разследването и правоприлагането.

Суверенитетът – отправна точка при противодействие на киберпрестъпността

Отправната точка за взаимодействието между националното правосъдие и международното сътрудничество е суверенитетът. Националният суверенитет на държавите е гарантиран от международното право. То включва правилото за ненамеса на една държава под никаква форма или причина във вътрешните или външни работи на друга държава. Прилагането на закона е изцяло в правомощията на суверенната държава – по правило правосъдието е приложимо в териториалните географски граници на държавата. Държавите следва да се въздържат да оказват натиск върху други държави относно поведението и правомощията на правосъдните и правораздавателните им органи. Специфични дейности, като арести, разследвания и акции на територията на друга държава, не могат да бъдат извършвани освен при наличие на съответен договор и съгласието на страните.

Разбира се, не всички престъпления са винаги в териториалната юрисдикция, при което международното право признава набор от общи принципи за извънтериториална юрисдикция на криминалните въпроси. Тези общи принципи са изведени от националните закони и международните договори. Общото в тях е смисълът на изискванията за достатъчна свързаност и естествена връзка между нарушението и държавата, където да се приложи законодателството. Важно е да се подчертае, че такова законодателство не разрешава автоматично „физическото" присъствие за дейности по разследване и операции на територията на другата държава – в подобни случаи е необходимо наличието на съответното съгласие.

Международна правна помощ

С цел управление на процеса на съгласие за провеждане на дейности по разследване и операции по правоприлагане на територията на друга държава, съществуват както правни, така и неформални договорености между държавите, създадени на двустранна или многостранна основа. Такъв пример е екстрадирането на заподозрени в престъпление, т.е. предаване на извършителя на друга държава. В допълнение към екстрадирането, основните средства на международното сътрудничество включват помощ при събиране на доказателства и договорености за международен трансфер на осъдени хора.

Екстрадирането се определя като официален процес на изискване, от една страна, да се предаде обвиняем или осъден за престъпление с цел извършване на съдебен процес или излежаване на присъдата в изискващата страна. Обичайното международно право не съдържа задължения за екстрадиране. Договореностите са обикновено на базата на двустранни или многостранни договори на принципа реципрочност – обещание от едната страна на другата за предоставяне на същия вид помощ, ако се поиска такава. С цел избягване на пропуски основният принцип тук е „екстрадирай или процедирай". По подобен начин процедурите за взаимноправна помощ се основават на

двустранни или многостранни договори. Екстрадирането и взаимноправната помощ може да са общо присъстващи в договорите или с определен (ограничен) обхват на приложение. Много често, където такива договори съществуват, процедурата за привеждането им в изпълнение е заложена в националните закони. Друга практика е националният закон да определя такова международно сътрудничество.

Тъй като една от основните цели при взаимноправната помощ е да се доставят доказателства за разследването и съда, процедурата е обвързана по-нататък с националното право. Доказателствата, придобити извън граница – често от помолената страна чрез нейните процедури, – трябва да отговорят на изискванията на правилата за набиране на доказателства от молещата страна. Алтернатива и развитие на взаимно правната помощ е принципът на *взаимното признаване* в криминалното разследване. Този принцип опростява и ускорява процедурата по разследването на киберпрестъпления.

Допълнително към посочените форми за международно сътрудничество може да се посочи, че част от извънтериториалното разследване може да бъде осъществено чрез неофициално междуполицейско сътрудничество. То може да бъде проведено преди официалните действия за договорената взаимноправна помощ или за улесняване на нейното прилагане. Ефективността на неформалното полицейско сътрудничество се определя от влиянието на два основни фактора:

- молбата за неформално полицейско сътрудничество да не се възприема от помолената страна като опит за извънтериториално разследване без изричното съгласие на домакина;
- всички събрани доказателства да отговарят на стандартите на молещата страна по отношение на събирането и съхранението им.

Официално международно сътрудничество при противодействие срещу киберпрестъпността

Отправна точка при оценка на ефективността на официалното международно сътрудничество при противодействие срещу киберпрестъпления е обхватът на сътрудничеството. Докато юрисдикционните предпоставки в международните и регионалните инструменти визират определени нарушения, извършени според тях, условията на международното сътрудничество могат да имат по-широк обхват. Предпоставките за международно сътрудничество варират от киберпрестъпления, престъпления с компютърна информация или с информация и информационни технологии до събиране на електронни доказателства за всякакви престъпления. Механизмите на международното сътрудничество обаче могат да имат и доста по-широк контекст – като пример, ако страната участва в организации и договори на двустранно и многостранно ниво. Също така, в зависимост от характера на престъплението, то може да попадне под различни видове правни механизми – не само тези, отнасящи се до киберпрестъпления. И накрая трябва да се подчертае, че незадължителните международни инструменти не могат да поставят същата (по ефективност) правна основа за международно сътрудничество, както задължителните – за сравнение рамкови програми и закони.

Често задължителните и незадължителните международни инструменти съдържат клаузи за екстрадиране на извършителите на престъпленията, изброени в тях. Екстрадирането е поставено под условности в зависимост от „двойствената криминалност" и сериозността на нарушението. Използваните инструментите определят, че молбата за екстрадиране може да бъде отказана, ако се счете, че противоречи на

националните закони, засяга политическата стабилност или националната сигурност, суверенитет или обществения ред.

В прилаганите инструменти се определя ред и средствата за комуникация, подаването на искания при спешни случаи, изискванията към сигурността на комуникацията и начина и времето за последващо предаване на искане. Някои конкретни особени условия на международното сътрудничество при разследване на киберпрестъпления могат да включват: спешно съхраняване на запазените компютърни данни; спешна разкриване на запазените данни за трафика; взаимопомощ при събиране на данни от трафика в реално време; взаимопомощ при прехващане на съдържанието на данните. Тези условия важат не само за киберпрестъпленията, но и за престъпленията като цяло.

Някои страни разполагат в националното си право с механизми за взаимно правна помощ и екстрадиране при киберпрестъпления, като по-често съществуват тези за екстрадирането. В повечето законодателства не се визират специално киберпрестъпленията. Липсата на национално законодателство не пречи на страните да си сътрудничат при случаи на киберпрестъпления. Въпросите по международното сътрудничество могат да бъдат решени с национални механизми – изпълнителни заповеди или административни политики.

За международните киберпрестъпления се използват по-често формалните (официалните) механизми за сътрудничество, отколкото другите форми. Според направено изследване[4] в глобален мащаб 60% от държавите не са страна по никакъв инструмент срещу киберпрестъпленията. Понастоящем молби за сътрудничество с такива страни следва да бъдат правени чрез традиционния двустранен метод или на базата на реципрочността. Това обаче може да се окаже неефективно в случаи, които изискват спешно съхраняване на запазените компютърни данни, поради неяснота дали това е част от двустранната договорка или липсата на такива мерки в националната процедура препятстват подобни действия.

Употребата на международното сътрудничество за разследване на киберпрестъпленията може да срещне предизвикателства относно еквивалентността на инкриминирането (криминализирането). Едно от изискванията в международното сътрудничество е *двойствената криминалност*. Принципът на двойствената криминалност гласи, че актът, за който молещата страна иска съдействие, трябва да е престъпление според законите на помолената за съдействие страна. Някои киберпрестъпления може да са криминализирани в една страна, а в друга – не. Следователно същите не отговарят на принципа за двойствено инкриминиране. От друга страна, двойствената криминалност има важна роля в защитата на държавния суверенитет при прилагането на закона и при самите съдебни дела. За международното сътрудничество е важно още установяването на прагове на сериозност на престъплението. Двойствената криминалност е необходимо изискване както за екстрадиране, така и за взаимно правна помощ.

Неофициално (неформално) международно сътрудничество при противодействие срещу киберпрестъпността

Според резултатите от проведено изследване инициативите за неофициалното сътрудничество предоставят важен потенциал за по-бързо реагиране в случаи на раз-

---

[4] Marko Gercke. Understanding Cybercrime: Phenomena, Challenges and Legal Response, 2012.

крити киберпрестъпления, а също така и анализът на механизмите на официалното и неофициалното сътрудничество не може категорично да определи дали същите предлагат достатъчно ниво на глобално сътрудничество. За повишаване на ефективността на международното сътрудничество е необходимо да се преодолеят различни предизвикателства, като например липса на определено време за отговор при събиране на електронни доказателства.

В допълнение на формите на официално сътрудничество за извънтериториално прилагане на закона се използват формите на неофициалното сътрудничество. Най-често преди официалното сътрудничество част от извънтериториалното разследване може да бъде осъществено чрез неофициално междуполицейско сътрудничество.

Неофициалното сътрудничество при разследване на киберпрестъпления с международен характер изисква създаване на добри комуникационни канали и надеждно оповестяване. Такава роля могат да изпълняват лицата за контакт със задача да осигуряват технически съвети, запазване на данни, събиране на доказателства, осигуряване на правна помощ, локализиране на заподозрени и др. Най-често точките за контакт се установяват в полицията или в правосъдните органи на отделните страни. Съществуват също така няколко мрежи за неофициално киберсътрудничество, като например между страните, подписали Конвенцията за киберпрестъпления на Съвета на Европа, или между страните от Подгрупа за технологични престъпления на G8.

Неофициалното сътрудничество на национално ниво протича най-често при наличието на някаква форма на договореност между страните и с ангажимента на компетентен и добре организиран партньор. При него са важни контактите, създадени чрез международните организации и институции, частните мрежи и правоналагащите органи. За нуждите на успешното разследване необходима стъпка е създаване на международни полицейски канали за обмен на информация. В неофициалното сътрудничество често съществуват ръководства и протоколи, включително „неписани" правила.

Друг важен момент в неофициалното сътрудничество е свързан с това, кой е назначен да взима решение за дейностите по сътрудничеството. Практиките показват различни варианти на приложение: от редови служител до началник на отделение за противодействие на киберпрестъпленията и от съдебен следовател до висш служител в Министерство на правосъдието.

Като обобщаващ извод може да се каже, че като цяло липсва достатъчно пълна и ефективна обща политика за изграждане и използване на форми за официално и неофициално сътрудничество между страните при разследване и правоприлагане срещу киберпрестъпления. В същото време общата липса на политика за сътрудничество не възпира държавите да определят точно какъв вид помощ им е необходима при разследване на киберпрестъпления. Като доказателство за това може да се посочи практиката правни и технически съвети да се обменят почти ежедневно между партньорите.

Използвана литература

Георгиев, В. Противодействие срещу киберпрестъпността. София, Авангард, 2014.
Marko Gercke. Understanding Cybercrime: Phenomena, Challenges and Legal Response, 2012.