IT4Sec Reports 148
http://dx.doi.org/10.11610/it4sec.0148

Локализмът в киберсигурността – мисия невъзможна

Венелин Георгиев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, октомври 2023

Венелин Георгиев, Локализмът в киберсигурността – мисия невъзможна, IT4Sec Reports 148 (септември 2023), http://dx.doi.org/10.11610/it4sec.0148

IT4Sec Reports 148 „Локализмът в киберсигурността – мисия невъзможна" Широкоспектърни концепции каквито са концепциите за локализъм и детериториализация могат успешно да бъдат използвани за изследване на специфични обекти какъвто е киберсигурността, разглеждана като функция на киберпрестъпленията. С помощта на методите за анализ и синтез се извеждат предизвикателствата, които детериториализацията поставя пред стратегическото управление на киберсигурността. Обобщаването на тези предизвикателства дава възможност за построяване на триъгълника на противоречията, който обяснява тезата за това, че при съвременните характеристики на киберпространството, „локализма“ се превръща в мисия невъзможна, а „детериториализацията“ извежда проблеми, касаещи киберсигурността, за които към настоящия момент няма решение.

Ключови думи: локализъм, детериториализация, киберпространство, киберсигурност, киберпрестъпност, триъгълник на противоречията

IT4SecReports 148 “Localism in cybersecurity – mission impossible”. Broad concepts such as the concepts of localism and deterritorialization could be successfully used to study specific objects such as cyber security as a function of cybercrime. Using the methods for analysis and synthesis, the challenges that deterritorialization poses to the strategic management of cyber security are brought out in the study. Summarizing these challenges allows the construction of the triangle of contradictions, which explains the thesis for the modern characteristics of cyberspace, where localism becomes a mission impossible, and deterritorialization raises cybersecurity problems that still have no particular solution.

Keywords: localism, deterritorialization, cyberspace, cybersecurity, cybercrime, triangle of contradictions

Редакционен съвет

Председател: акад. Кирил Боянов
Редактори: д-р Стоян Аврамов, проф. Генадий Агре, доц. Кирил Алексиев, проф. Даниела Борисова, проф. Венелин Георгиев, проф. Величка Милина, доц. Златогор Минчев, доц. Георги Павлов, проф. Тодор Тагарев, доц. Велизар Шаламанов
Отговорен редактор: Наталия Иванова

© Венелин Георгиев

ISSN 1314-2119

ВЪВЕДЕНИЕ

Стратегическото управление на киберсигурността в значителна степен се повлиява от развитието на технологиите и мрежите, изграждащи киберпространството. В същото време то може да бъде изследвано с помощта на теоретичните концепции за локализъм и детериториализация. Обединявайки двете гледни точки може да се формулира хипотезата, че в процеса за развитие на киберпространството концепцията за локализма ще бъде изместена от концепцията за детериториализация. Като следствие може да се очаква, че пред киберсигурността ще възникват предизвикателства, свързани с противодействието срещу киберпрестъпността. С помощта на методите за анализ и синтез тези предизвикателства могат да бъдат изведени и адресирани към стратегическото управление на киберсигурността и неговите проблеми.

Локализъм, детериториализация, киберпространство и киберсигурност в полето на дефинициите

Изясняването на смисъла на понятията, на тяхната същност и съдържание, както и на съществуващите връзки и зависимости между описваните с тяхна помощ процеси и състояния се нуждае от дефинирането на тези понятия. Колкото по-сложни и по-комплексни са дадени понятия, толкова е по-сложна задачата за тяхното дефиниране по начин, който да ги обедини в една изследователска концепция. В случая изследователската концепция се изгражда около установяване на връзки и закономерности между локализма и детериториализацията, пренесени в областта на киберпространството и определящи особеностите на киберсигурността и противодействието срещу киберпрестъпността.

Същността на термина локализъм, описван в различни литературни източници като пример, може да бъда обединена в следните три определения:

- локализмът представлява система от норми в средата на благородството, която е действала през 15-17 век в Русия, за която е характерно, че раздаването на привилегиите на болярите се е извършвало на княжевската маса на базата на значението и положението на благородниците и генеалогичното положение на всеки представител на техните родове;[1]
- локализмът представлява разбиране за това, че услугите трябва да бъдат осигурявани и контролирани, а благата трябва да бъдат произвеждани и купувани в рамките на ограничена област и в полза на потребителите от тази област;
- локализмът описва съвкупност от политически философии, които приоритизират местното: в производството и потреблението на блага; в контрола на управлението; в акцентирането върху местната история, култура и идентичност.[2]

Търсейки ползите от локализма в социално-икономически план следва да се отбележи, че[3,4]:

- при локализма местният бизнес плаща данъци, които се използват от местната общност за финансиране построяването на училища и болници, както и за поддържане на други публични услуги;

[1] „Какво е локализъм? Определение, същност, въвеждане и анулиране в Русия," 2019, https://bg.puntomarinero.com/what-is-localism-definition-essence/.
[2] Cambridge Dictionary, 2023, https://dictionary.cambridge.org/dictionary/english/localism.
[3] Kurland, K., Hill, D. The Localism Movement: Shared and Emergent Values, https://www.researchgate.net/publication/258088971_The_Localism_Movement_Shared_and_Emergent_Values
[4] Severn, C. Localism: theory and practice including a case study of the transition town movement, https://transitionnetwork.org/sites/www.transitionnetwork.org/files/ResearchPaper-LocalismAndTransition-ChloeSevern-March2013%20pdf.pdf

- при локализма е характерно тясно сътрудничество между местни банки, доставчици и т.н. Той подобрява координирането и интегрирането на публичните услуги.
- локализмът успява по достатъчно ефективен начин да удовлетворява потребностите на общността споделяйки разбирането, че колкото по-комплексно и по-разделено е обществото, толкова по-трудно е на централизираното ръководство да осигури за хората блага, отговарящи на техните потребности;
- локализмът изгражда сигурност и устойчивост за общността, стимулира иновациите, намалява разходите за управление на общността.

В основата на термина детериториализация стои негативното разбирането за понятието територия, което е свързано с граници, отношения между субекти, власт.[5] От своя страна териториализацията може да се разбира като начин да бъде взето решение законите на коя държава да бъдат приложени в конкретен случай.[6] От гледна точка на избраната изследователска концепция, териториализацията в киберпространството поставя въпроси като: кой трябва да управлява киберпространството, какви правила и регулации следва да бъдат спазвани в това пространство и т.н. Трудностите при намирането на отговори на горните въпроси идват от това, че самото киберпространство е „навсякъде и никъде“. То представлява съвкупност от взаимно свързани мрежи, включващо физически компоненти (технически устройства, кабели и др.) и дигитални компоненти (софтуер, протоколи и др.), които позволяват на потребителите да оперират с информация като използват свързани в мрежа компютри. Като следствие от изброените трудности и специфики на киберпространството, разбираемо изглежда приложението на детериториализацията като оперативна и управленска концепция в това пространство, за което в момента е характерна повсеместна, глобална свързаност и липсата на всякакви географски и физически граници.

Третият компонент от конструкцията на изследователската концепция е киберпространството. Като понятие то също може да се определи с помощта на множество определения, зависещи от отчитаната гледна точка. Като пример за подобни определения могат да бъдат дадени следните:

- киберпространството представлява съвкупност от компютърни устройства, свързани в мрежа, в които се съхранява и използва информация в електронен вид, а също така се извършва комуникационен процес;
- киберпространството представлява нова вселена, или още, паралелна вселена, създадена и поддържана с помощта на световните компютърни и комуникационни мрежи;
- в съдържанието си киберпространството включва всички компютърни мрежи в света, както и всичко, с което тези мрежи са свързани и което те управляват по кабел, чрез оптични влакна и по безжичен път;
- киберпространството представлява комплексна среда, появила се вследствие от взаимодействието на хора, софтуер и услуги, които предоставя чрез използване на технически средства и мрежи, които са свързани към интернет.

Търсейки обобщение на характеристиките на киберпространството, имащи отношение към неговата сигурност, следва да бъдат отбелязани:

- липсата на всякакви физически и географски граници, като следствие от което е факта, че информацията, която се създава, обработва, предава и съхранява в компютърните мрежи може да бъде достъпвана и атакувана от разстояние без да

[5] „Детериториализация,“ Енциклопедия на постмодернизма, 2023, https://kato.koshachek.com/articles/deteritorizacija-enciklopedija-na-postmodernizma.html.
[6] “Deterritorialization,” Wikipedia, 2023, https://en.wikipedia.org/wiki/Deterritorialization.

е необходимо физическото присъствие на киберпрестъпника на мястото на престъплението. Глобалната свързаност като основна характеристика на киберпространството от една страна предоставя възможности за потребителите, а от друга страна е причина и източник за заплахите за сигурността на тези потребители;

- заплахите в киберпространството са толкова разнообразни, колкото разнообразно е самото киберпространство и тези заплахи произтичат от природата на компютърните мрежи, тяхната взаимна свързаност и мащаб, скорост за предаване на информацията и т.н.

Последният, четвърти компонент от изследователската концепция е киберсигурността. Терминът киберсигурност е използван за първи път през 1996 г. и бързо се превръща в модерна дума, която плаши със своята неопределеност, доколкото зад нея могат да стоят неограничен брой въпроси и проблеми на сигурността, започващи от техническата област и завършващи до областта на законодателството. При всички положения сериозните дискусии в областта на киберсигурността изискват на първо място въвеждане и използване на общи дефиниции. Като примери за такива могат да бъдат дадени следните:

- киберсигурността включва в себе си проблемите на сигурността, свързани с интернет и други компютърни системи и мрежи, а също така и техническите и нетехническите способи за решаване на тези проблеми;
- киберсигурността представлява съвкупност от политики, средства, концепции, ръководства, действия, обучение, добри практики и технологии, които могат да се използват за защита на киберпространството, организациите и потребителите. В съдържанието на организациите и потребителите се включват свързаните компютърни устройства, инфраструктурата, приложенията, услугите, телекомуникационните системи и информацията, която се създава, съхранява и обработва в киберпространството;
- Международната организация за стандартизиране (ISO) дефинира киберсигурността като запазване на конфиденциалността, интегритета и достъпността на информацията в киберпространството.

Киберсигурността може да бъде извеждана и оценяване на базата на различни характеристики, т.е. тя може да бъде функция на различни променливи. В настоящото изследване киберсигурността се разглежда като функция на способностите за разкриване, разследване и правоприлагане в случаи на киберпрестъпления, или казано по-общо, на способностите за противодействие срещу киберпрестъпността.

При така дефинираните понятия изследователската концепция се изправя пред следните въпроси:

- възможно ли е приложението на принципите на локализма в киберпространството и какви последствия може да има това за киберсигурността и за ползите на потребителите;
- какви са предизвикателствата пред сигурността на киберпространството в контекста на принципа за детериториализация.

Да средата на миналия век размерите и мащабите на компютърните мрежи са ограничени и не се характеризират с транснационален и още по-малко с глобален обхват. Като следствие, свързано с киберсигурността, основната част на киберпрестъпленията са с национално значение и почти не се говори за киберпрестъпления от международен характер. При тези условия не представлява трудност в случай на извършено киберпрестъпление да се определи релевантната юрисдикция и кои норми на материалното и процесуалното право да

бъдат използвани в процеса на разкриване, разследване и правоприлагане. От друга страна, при това състояние на техническите възможности на компютърните мрежи в ограничен мащаб се използват възможностите за свързаност и обмен на информация между потребителите. Като обобщение може да се каже, че ограниченият мащаб на компютърните мрежи прави възможно прилагането на концепцията за локализъм спрямо противодействието срещу киберпрестъпността в рамките на търсенето на сигурност в киберпространството. Като стратегическа управленска концепция локализмът е по-детерминиран и конкретен, което допринася за постигане на по-ефективно противодействие срещу киберпрестъпността и по-високо ниво на киберсигурност.

С развитието на технологиите и нарастването на мащаба, обхвата и скоростта на обработваната информация в рамките на компютърните мрежи, както и за сметка на появата на глобални компютърни мрежи, в рамките на киберпространството концепцията за локализма бива изместена от концепцията за детериториализация. Новата концепция, базираща се на новите възможности на киберпространството, създава нови предизвикателства пред стратегическото управление на киберсигурността.

Предизвикателства пред стратегическото управление на киберсигурността, създадени от концепцията за детериториализация

Предизвикателствата пред стратегическото управление на киберсигурността, създавани от концепцията за детериториализация могат да бъдат изследвани с помощта на методите анализ и синтез. Това на практика означава на първо място да бъдат разгледани предизвикателствата от различни гледни точки като се посочат специфичните характеристики и след това да се направят обобщения, касаещи предизвикателствата като цяло от гледна точка на стратегическото управление на киберсигурността.

Анализът на предизвикателствата пред стратегическото управление на киберсигурността, създавани от концепцията за детериториализация се извършва от следните гледни точки:[7]

- *предизвикателства по отношение на общото разбиране за това какво представляват киберпрестъпленията, разглеждани като измерители на киберсигурността*.

Въпреки своята популярност терминът „киберпрестъпност“ не може да бъде еднозначно дефиниран и не може да бъде срещнат във всички речници, дори и в специализираните такива. Това прави киберпрестъпността нещо, което трудно се дефинира и в същото време нещо, за което много хора говорят. Основната причина, която затруднява единното дефиниране на киберпрестъпността са различията в законодателните стандарти на различните държави. Съществена особеност на киберпрестъпленията е, че те се проявяват във виртуална среда, наричана киберпространство, което допълнително затруднява определянето на това коя юрисдикция е в сила и кой точно законодателен стандарт да бъде прилаган в конкретния случай. Много често киберпрестъпникът и неговата жертва се намират на стотици и дори на хиляди километри един от друг, на територията на различни държави и континенти. Това прави възможно деянието да бъде инкриминирано в едната страна и да не бъде признато като престъпление в другата страна. В подобни случаи възникват въпроси от типа: законите на коя от двете страни да бъдат приложени или може ли да се преследва дадено лице за извършено престъпление в страна, в която то никога не е пребивавало. Друг проблем на адекватното дефиниране на киберпрестъпността е липсата на достатъчно статистически данни за нея. Най-често за случаи на киберпрестъпления докладват жертвите, при това на доброволен принцип, което е една от причините за ниския брой на известните

[7] Георгиев, В. *Противодействие срещу киберпрестъпността* (София: Авангард, 2022), https://edubooks.bg/all-products/categorys-listing/category/91-91ns.

инциденти. Изброените аргументи за трудностите пред общото дефиниране на киберпрестъпността увеличават значимостта на въпроса защо всъщност е толкова важно наличието на общоприето определение за този термин. Възможни са следните отговори:

- за да се улесни общуването между ИТ персонала, потребителите, жертвите, органите за разследване и разкриване, прокурорите и съдиите;
- за да стане възможно събирането и натрупването на статистическа информация за киберпрестъпността, на базата на която да се анализират престъпни модели и тенденции;
- за по-адекватно разпределяне на инвестициите и за планиране на начините за противодействие срещу киберпрестъпността;
- за информиране и обучение на хората по проблемите, свързани със заплахите, идващи от киберпрестъпността;
- за повишаване на ефективността на мерките за превенция, разбирането на различните видове киберпрестъпления, къде и кога те се случват, кой е въвлечен в тях: всичко това е необходимо за разработването на план за превенция на киберпрестъпността.

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 и множество различни класификационни модели 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 киберпрестъпност се достига до определение, според което киберпрестъпността 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.

Многообразието в определенията за понятието киберпрестъпност като измерител на киберсигурността е в следствие на характеристиките на киберпространството и в унисон с концепцията за детериториализация. Като общ резултат от тази зависимост е ниската ефективност на противодействието срещу киберпрестъпността и ниското ниво на киберсигурност.

- *предизвикателства по отношение на прилагането на стратегически подход за създаване на киберсигурност чрез противодействие срещу киберпрестъпността*

Въпросите, свързани с киберсигурността и с противодействието срещу киберпрестъпността са изключително комплексни и изискват прилагането на стратегически подход при търсенето на подходящ отговор. Стратегията за противодействие срещу киберпрестъпността без съмнение следва да бъде неразделна част и да подпомага цялостната стратегия за киберсигурност. Отделните страни могат да избират между създаване на собствени уникални стратегии за противодействие срещу киберпрестъпността или адаптиране и прилагане на вече съществуващи подобни стратегии. Използването на съществуващи стратегии за противодействие срещу киберпрестъпността от една страна води

до спестяване на време и усилия, а също така създава условия за използване на опита на доказано добри практики, но от друга страна може да се превърне в източник на проблеми за страната, решила да заимства една или друга стратегия за противодействие срещу киберпрестъпността. В основата на тези потенциални проблеми стои невъзможността за осигуряване на достатъчни като количество и качество ресурси за прилагане по достатъчно ефективен начин на избраната стратегия. Страните с развити икономики могат да си позволят повишаване на нивото на киберсигурност като прилагат в практиката по-гъвкави способи от типа на внедряване на скъпоструващи защитни технически системи. За останалите страни като възможност остава прилагането на опростени стратегии за създаване и поддържане на ниво на киберсигурност. Характерният за съвремието силно преобладаващ международен характер на киберпрестъпността прави от изключителна важност в борбата срещу същата степента на хармонизиране на стратегиите на различните страни. От своя страна самата хармонизация следва да бъде съобразена с регионалните, местните (локалните) особености, изисквания и възможности. Стремежът към унифицираност на стратегиите за противодействие срещу киберпрестъпността води към подчиняване на тяхното съдържание на следните пет опори:

- ефективни материални и процесуални правни норми за противодействие срещу киберпрестъпността;
- технически и процедурни мерки за противодействие срещу киберпрестъпността;
- организационна структура, осигуряваща ефективно противодействие срещу киберпрестъпността;
- изграждане на потенциал за противодействие срещу киберпрестъпността и обучение на потребителите;
- изграждане на достатъчно ефективно международно сътрудничество в интерес на противодействието срещу киберпрестъпността.

По отношение на стратегическия подход към управлението на киберсигурността, концепцията за детериториализация поставя следните конкретни предизвикателства:

- не всички държави разполагат с достатъчно ефективни стратегии за киберсигурност, а при една не малка част от страните такива стратегии изобщо липсват;
- степента на съгласуваност между стратегиите за противодействие срещу кибепрестъпността на различните държави е ниска и се основава на различни фактори, от които един от най-значимите е суверенитетът на отделните страни;
- опитите за унифициране на националните стратегии за противодействие срещу киберпрестъпността на базата на директиви на международни организации не срещат нужното разбиране и усилия от страна на отделните държави.

Горните причини снижават ефективността на стратегическото управление на киберсигурността и отново в основата стои концепцията за детериториализация, характерна за съвременното състояние на киберпространството.

- *предизвикателства по отношение на способностите за разкриване, разследване и правоприлагане при киберпрестъпления*

От направени изследвания става ясно, че между петдесет и деветдесет процента от киберпрестъпленията, с които полицията се е сблъсквала, представляват престъпления с международен характер. В същото време, по-голямата част от тези престъпления достигат до знанието на полицията чрез показанията на жертвите, по-често в лицето на частни лица. По този начин се оказва, че киберпрестъпността съществува навсякъде, но най-често се отчита и на нея се противодейства на местно (локално) ниво. При различните страни се

наблюдава значителна разлика в капацитета на полицията в разследването на киберпрестъпления.

На базата на резултатите от проведено изследване се констатира, че над деветдесет процента от киберпрестъпленията достигат до знанието на полицията в резултат на доклади от лица и фирми, които са станали жертва на киберпрестъпление. Докладваните случаи на киберпрестъпления са изключително малка част от общия брой извършени престъпления от този тип. Липсата на достатъчен брой доклади за киберпрестъпления до правоохранителните органи се дължи на множество фактори, в това число: недостатъчно публично доверие във възможностите на полицията при провеждането на разследванията; липсата на информация за механизмите за докладване; срамът и смущението от това, че лицата са станали жертви; рискът за фирмите от разваляне на тяхната репутацията; невъзможност за преценка от страна на жертвата за наличие на киберпрестъпление.

Предизвикателствата, отправяни от концепцията за детериториализация пред киберсигурността, свързани със способностите за разкриване, разследване и правоприлагане в случаи на киберпрестъпление, имат следния произход:

- различни нива на способности за разкриване, разследване и правоприлагане при киберпрестъпление, които изграждат и използват отделните страни;
- различен инструментариум за разкриване и разследване на киберпрестъпления. По-голямата част от страните използват инструментите, характерни за разкриване и разследване на конвенционални престъпления и само малка част от страните използват специализирани инструменти, отговарящи на спецификата на киберпрестъпленията. В някои от страните отсъства правната възможност за прилагане на специализирани средства за разкриване и разследване на киберпрестъпления;
- различни нива на подготовка на служителите, натоварени със задълженията по разкриване, разследване и правоприлагане при киберпрестъпления;
- различен мащаб и различни нива на ефективност на публично-частното партньорство при разкриване и разследване на киберпрестъпления.

Горните предизвикателства са следствие от концепцията за детериториализация, приложима към настоящия момент в киберпространството. Същите снижават ефективността при разкриване, разследване и правоприлагане в случаи на киберпрестъпления с международен характер, а от там и на нивото на киберсигурност като цяло.

- предизвикателства по отношение на превенцията на киберпрестъпленията

Превенцията на киберпрестъпността се отнася до стратегиите и мерките, които имат за цел да намалят риска, измерен чрез вероятността за потенциалните киберпрестъпления и техния евентуален вреден ефект върху хората и обществото като цяло чрез намеса, която влияе върху разнообразните случаи на киберпрестъпност. Киберпрестъпленията и концепцията за детериториализация поставят конкретни предизвикателства пред криминалната превенция. Сред тези предизвикателства могат да бъдат посочени:

- нарастващо използване на онлайн приложения, които водят до нарастване на броя на потенциалните жертви;
- относителна готовност на хората да рискуват в интернет;
- възможност за анонимност или смяна на идентичността;
- международен характер на повечето киберпрестъпления;
- бързо развитие и навлизане на иновациите в престъпността.

По данни от проведено изследване около четиридесет процента от участващите страни разполагат с национално законодателство или политика относно превенция на киберпрестъпността. Други двадесет процента от страните посочват, че са в период на изготвяне на подобна специфична законова рамка. Преобладаващата част от страните със съществуваща нормативна база и политика за превенция на киберпрестъпността са от Европа и Северна Америка, по-малко са тези от Африка, въпреки че около четиридесет процента от страните там са в процес на изготвяне на такъв правно регулиращ инструмент. Общото обаче в случая е фактът, че повече от половината от всички участващи държави потвърждават, че съществуването на национална политика и законодателство за превенция на киберпрестъпността създава възможности за изграждане на потенциал за справяне с киберпрестъпленията.

Държавите, които разполагат с изготвени закони за превенция на киберпрестъпността смятат, че самите закони обикновено се създават с цел да:

- организират и координират правната страна на превенцията на киберпрестъпността;
- изградят достатъчно ефективна институционална система;
- разпределят ролите и отговорностите за различните аспекти на превенцията на киберпрестъпността
- осигурят информация за потребителите, техническия персонал и хората, които вземат решенията.

Различните страни ползват различни практики по отношение на превенцията на киберпрестъпността. В прилагането на тези практики участие вземат различни правни агенции, държавни институции, изследователската общност и организации от частния сектор. В някои страни се обръща особено внимание на банковия сектор, сигурността в интернет, изготвянето на обучения в сферата на киберзащитата в сътрудничество с неправителствени организации на територията на училищата и не на последно място на ролята на правните агенции, участващи в редица конференции и други форуми, засягащи киберпрестъпността.

Предизвикателствата пред превенцията на киберпрестъпността могат да бъдат обобщени като недостатъчен брой на страните, подхождащи стратегически към проблемите на превенцията и съществените различия в организацията и инструментите на превенцията. Посочените предизвикателства са следствие от концепцията за детериториализация и същите оказват негативно влияние върху изграждане и поддържане на състояние на киберсигурност.

- *предизвикателства по отношение на способностите за международно сътрудничество при противодействие срещу киберпрестъпността*

Киберпрестъпленията далеч не са първата форма на престъпност, изискваща глобално противодействие. През изминалите години глобални усилия в противодействието са прилагани срещу тероризма, търговията с наркотици, международната организирана престъпност и т.н. От друга страна безспорен е фактът, че киберпрестъпленията днес поставят уникални предизвикателства пред международното сътрудничество по пътя на противодействието срещу тях.

Отправната точка за взаимодействието между националното правосъдие (юрисдикция) 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. Прилагането на закона е изцяло в правомощията на суверенната държава - по правило правосъдието е приложимо в териториалните географски граници на държавата. Държавите трябва да се въздържат да оказват натиск на други държави относно поведението

и правомощията на правосъдните и правораздавателните им органи. Разбира се не всички престъпления са винаги в териториалната юрисдикция, при което международното право признава набор от общи принципи за извън териториална 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.

Кога и как може да се определи, че киберпрестъпленията имат международен характер? При търсенето на отговор на този въпрос, според ООН, отправните точки могат да бъдат следните:

- киберпрестъпление, извършено на територията на повече от една държава;
- киберпрестъпление, извършено в една държава, когато същото е подготвено, планирано и управлявано от територията на друга държава;
- киберпрестъпление, извършено в една държава, когато е подготвено от организирана група, действаща в повече от една държави;
- киберпрестъпление, извършено в една държава, но нанесло значителни вреди на друга държава.

За международните киберпрестъпления се използват по-често формалните (официалните) механизми за сътрудничество, отколкото другите форми. Според изследването, в глобален мащаб 60% от държавите не са страна по никакъв инструмент за международно сътрудничество в борбата 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 като „спешно съхраняване на запазените компютърни данни" поради неяснота дали това е част от двустранната договорка или липса на такива мерки в националната криминална процедура.

Употребата на международното сътрудничество за разследване на киберпрестъпленията може да срещне предизвикателства, касаещи детериториализацията, относно еквивалентността на инкриминирането (криминализирането). Едно от изискванията в международното сътрудничество е двустранната криминалност. Принципът на двустранната криминалност гласи, че актът, за който молещата страна иска съдействие трябва да е престъпление според законите на помолената за съдействие страна.

В допълнение на формите на официално сътрудничество за извън териториално прилагане на закона се използват формите на неофициалното сътрудничество. Най-често преди официалното сътрудничество, част от извън териториалното разследване може да бъде осъществено чрез неофициално, междуполицейско сътрудничество или сътрудничество между агенциите за сигурност.

Неофициалното сътрудничество изисква създаване на добри комуникационни канали и 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 са установени в полицията, агенциите и правосъдните органи на отделните страни. Съществуват също така няколко мрежи за неофициално киберсътрудничество, като пример между страните, подписали Конвенцията за киберпрестъпления на Съвета на Европа, или между страните от Подгрупата за технологични престъпления на G8.

Неофициалното сътрудничество на национално ниво протича най-често при наличието на някаква форма на договореност между страните и на компетентен и добре организиран партньор. При него са важни контактите, създадени чрез международните организации и

институции, частните мрежи и право налагащите 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.

Тромавостта на процедурите на формалното международно сътрудничество, липсата на официализиране на формите за неформално международно сътрудничество и ниският брой на страните, участващи в споразумения за международно сътрудничество представляват предизвикателства пред противодействието срещу киберпрестъпността и създаване на състояние на киберсигурност. В основата на тези предизвикателства стоят принципи като суверенитет, юрисдикция, национално законодателство, присъщи на концепцията за локализъм, които следва да се съвместят с концепцията за детериториализация, идваща от особеностите на киберпространството, при което липсват всякакви географски и физически граници.

Следствия от липсата на възможност за локализъм и превъзходството на детериториализацията при стратегическото управление на киберсигурността

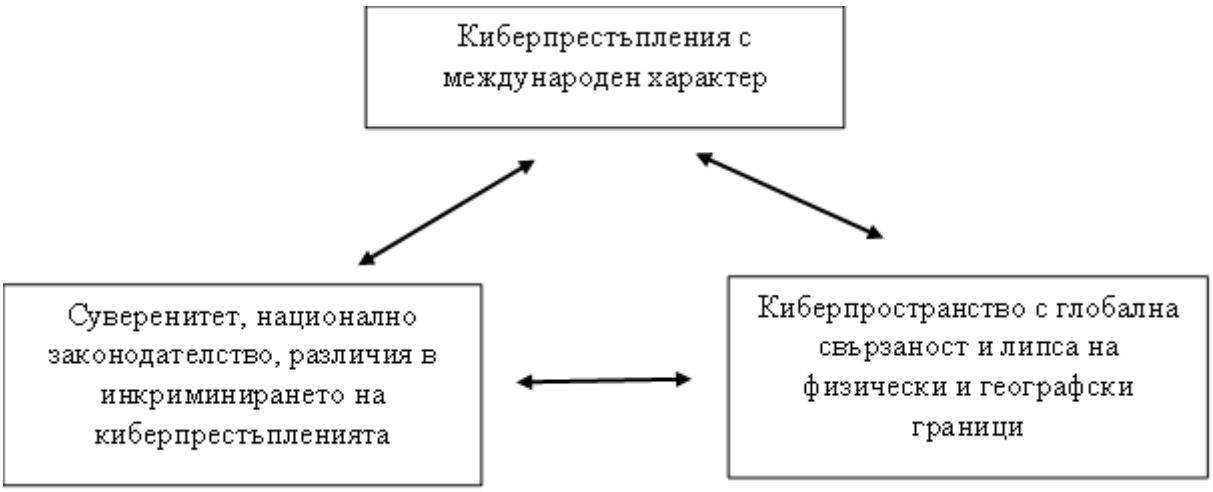
Изброените по-горе предизвикателства пред стратегическото управление на киберсигурността са следствие от противоречията между концепциите за локализъм и детериториализация и особеностите на киберпространството като среда за постигане на киберсигурност.

В Таблица 1 са представени резултатите от сравнителен анализ на възможностите за противодействие срещу киберпрестъпността в съвременни условия в различните области, представени по-горе.

Таблица 1. Резултати от сравнителния анализ

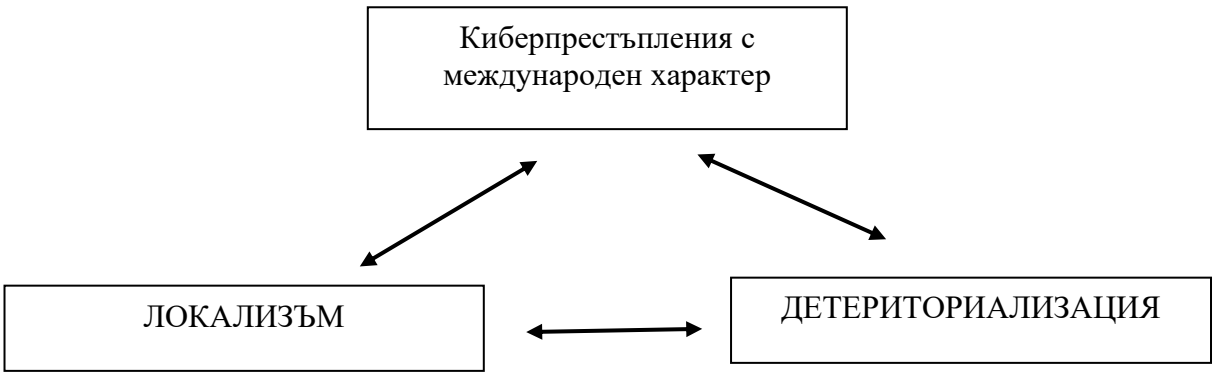
Концепция/Област на противодействие	Локализъм	Детериториализация
1. Общо разбиране за същността и особеностите на киберпрестъпността	Наличие на национални (локални) модели за класифициране на киберпрестъпленията	Опити за извеждане на общо определение и класификация на киберпрестъпленията
2. Стратегически подход за управление на киберсигурността	Наличие на отделни стратегии на ниво държава не всички интегриращи изискванията на международните документи	Липса на единен стратегически подход; наличие на страни, които изобщо не разполагат със стратегии
3. Способности за разкриване, разследване и правоприлагане	Индивидуално ниво на способности за разкриване и разследване на киберпрестъпления в отделните държави	Липса на общ пакет от способности за разкриване и разследване на международни киберпрестъпления
4. Превенция на киберпрестъпността	Индивидуални национални подходи за структуриране на стратегиите за превенция	Липса на единно стратегия за превенция на киберпрестъпността
5. Международно сътрудничество при противодействие срещу киберпрестъпността	Различия в национални разбирания и усилия за участие във форми за международно сътрудничество	Нисък броя на държавите, прилагащи на взаимна база инструменти за международно сътрудничество

Резултатите от сравнителния анализ, показан в Таблица 1 дават основание да бъде структуриран т.нар. триъгълник на противоречията (виж Фигура 1).



Фигура 1. Триъгълник на противоречията

От Фигура 1 се вижда, че характеристики като суверенитет, национално законодателство и различия при инкриминирането на киберпрестъпленията влизат в противоречие с общите характеристики на киберпространството от гледна точка на възможностите за противодействие срещу международната киберпрестъпност в стремежа за постигане на киберсигурност.



Фигура 2. Трансформиран триъгълник на противоречията

При трансформиране на Фигура 1 с помощта на терминологията за локализъм и детериториализация са достига до т.нар. трансформиран триъгълник на противоречията (виж Фигура 2).

Като извод може да се каже, че развитието на технологиите и мрежите в киберпространството налагат разбирането за отпадане на ограниченията по отношение на глобалната свързаност на потребителите. В следствие от това концепцията за локализъм се

измества от концепцията за детериториализация, при което възникват предизвикателства пред разкриването, разследването и правоприлагането при международни киберпрестъпления. Голяма част от тези предизвикателства към момента не са решени и като следствие не може да бъде постигната желаната степен на киберсигурност за потребителите.

ЗАКЛЮЧЕНИЕ

От направеното изследване се вижда, че концепциите за локализъм и детериториализация могат да намерят приложение при извеждане на предизвикателствата пред стратегическото управление на киберсигурността. Развитието на технологиите и компютърните мрежи се превръща в причина за прехода от локализъм към детериториализация, с което се доказва още веднъж тезата, че технологическия прогрес освен, че осигурява предимства, създава и проблеми, голяма част от които към момента не са решени. Локълизмът в киберпространството се превръща в мисия невъзможна, но проблемите на детериториализацията от гледна точка на стратегическото управление на киберсигурността остават върху масата за решаване.

БИБЛИОГРАФИЯ

[1] Георгиев, В. *Противодействие срещу киберпрестъпността* (София: Авангард, 2022), https://edubooks.bg/all-products/categorys-listing/category/91-91ns.

[2] „Какво е локализъм? Определение, същност, въвеждане и анулиране в Русия,“ 2019, https://bg.puntomarinero.com/what-is-localism-definition-essence/

[3] Kurland K., Hill D. The Localism Movement: Shared and Emergent Values, https://www.researchgate.net/publication/258088971_The_Localism_Movement_Shared_and_Emergent_Values

[4] Severn C. Localism: theory and practice including a case study of the transition town movement, https://transitionnetwork.org/sites/www.transitionnetwork.org/files/ResearchPaper-LocalismAndTransition-ChloeSevern-March2013%20pdf.pdf

[5] „Детериториализация,“ Енциклопедия на постмодернизма, 2023, https://kato.koshachek.com/articles/deteritorizacija-enciklopedija-na-postmodernizma.html

[6] Cambridge Dictionary, 2023, https://dictionary.cambridge.org/dictionary/english/localism

[7] “Deterritorialization,” Wikipedia, 2023, https://en.wikipedia.org/wiki/Deterritorialization