ПОПОСКА Весна[1] **УДК: 343.9:004**

ПРАВНИ АСПЕКТИ НА САЈБЕР БЕЗБЕДНОСТА

Апстракт: Сајбер безбедноста претставува релативно понова област, која ги зафаќа речиси сите аспекти на современото живеење. Специфичната природа на сајбер просторот, неговата специфична структура и нематеријалност, го прават комплексен за обезбедување. На крајот од денот, првичната намера на сајбер просторот не беше тој да биде „обезбеден“ или уште помалку, контролиран.

Работите се променија и истиот денес претставува сензитивна и критична област, и Ахилова петица на современото општество. Еден од клучните аспекти на оваа проблематика е правната рамка и тешкотите за нејзина апликација. Целта на трудот е да обезбеди сеопфатен пристап кон проблематиката, со цел на понатамошно изнаоѓање на препораки и реални насоки за ефективно справување со заканите, пропорционално на потребите и барањата на демократските општества.

Клучни зборови: *меѓународно, казнено, право, политики, стратегија*

POPOSKA Vesna

LEGAL ASPECTS OF CYBER SECURITY

Abstract: Cyber security represents a relatively new area that covers almost all aspects of modern life. The specific nature of cyberspace, its specific structure and immateriality, make it complex field for security. At the end of the day, the original intention of cyberspace was not to be “secured” or controlled.Things have changed, and today it is a sensitive and critical area, it is the “Achilles’ heel” of the modern society. One of the key aspects of this issue is the legal framework and its application. The purpose of the paper is to provide a comprehensive approach to the problem, in order to find further recommendations and realistic guidelines to deal effectively with threats in proportion to the needs and requirements of democratic societies.

Key words: *international, criminal, law, policy, strategy*

[1] Меѓународен Универзитет Визион - Гостивар, Р. Македонија
Авторката е докторандка на Воената академија „Генерал Михаило Апостолски“ - Скопје

1. Вовед и поимно определување

Тргнувајќи од поимната определба и јазичниот метод на толкување како примарен за правната наука, современите речници терминот „сајбер“ го дефинираат како: „во врска со, или карактеристика на културата на компјутери, информатичката технологија, и виртуелната реалност: сајбер ера“ (Оксфорд речници онлајн речник), или како „на, во врска со, или оние кои вклучуваат компјутери или компјутерски мрежи (како интернет)“ (Merriam-Webster, онлајн речник). Во македонскиот јазик се користи терминот „сајбер“ како интернационализам. Многу често како заменски се употребува терминот „компјутерски“ но истиот не ја отсликува доволно комплексноста на темата - бидејќи „сајбер“ во целокупната смисла е многу повеќе од „компјутери“. Често се наметнува дилемата дали е тоа посебна петта димензија на војувањето или нова димензија на постоечките четири, а таквата аналогија е применлива соодветно и во другите сфери на човечкото живеење и делување. Во секој случај, тоа е област која се развива и менува не на дневна база, туку во дел од часот, минутата и секундата, и го држи светот во неизвесна динамика. Инаку, етимологијата на „сајбер” датира уште од старогрчки и значи „регулира“ или „управува“ (eng: governance)[2].

Овие појави најдобро ги опиша претседателот на САД, Барак Обама, кога изјави дека: „Економски просперитет на Америка, националната безбедност, нашите индивидуални слободи, зависат од нашата посветеност за обезбедување на сајбер-просторот и одржување на отворен, интероперативен, безбеден и сигурен интернет. Нашата критичната инфраструктура продолжува да биде изложена на ризик од закани во сајбер просторот, а нашата економија е повредена од кражба на нашата интелектуална сопственост. Иако заканите се сериозни и тие постојано се развиваат, верувам дека ако им се посветиме ефективно можеме да се осигураме дека Интернетот останува мотор за економскиот раст и платформа за слободна размена на идеи“[3].

Најсоодветната и наједноставната дефиниција на сајбер безбеднсота (барем според авторката на овој текст) е дадена во безбедносната стратегија на Европската Унија од 2013 година и гласи: „Сајбер-безбедноста вообичаено се однесува на заштитните мерки и активности кои може да се користат за заштита на сајбер доменот, како во цивилните, така и во воените области, од тие точки кои се поврзани со или преку кои може да им се наштети независни мрежи, информации и нивна

2) Kurbalija, J. Internet Governance 6th edition

3) Достапно на https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

инфраструктура[4]“. Тоа имплицира дека и правната рамка ќе биде, условно кажано, и „цивилна“ и „воена“ - и национална, и меѓународна.

2. Практични импликации

Комплесноста на виртуелниот сајбер простор и безбедносните закани кои од него произлегуваат, предизвикува реални ефекти во сите аспекти на секојдневното живеење. Често се наметнува прашањето дали виртуелниот простор може да биде „место на злосторството“ или само алатка за негово извршување. За жал, и двете опции се возможни. Енормно брзиот технолошки напредок колку што го олесни живеењето и ги забрза економските процеси и глобализацијата, толку го направи светот во кој живееме поранлив. Безбедносно гледано, сајбер просторот е новата Ахилова петица - или подбро кажано, hic sunt leones („тука се кријат лавови“ -фигуративно, латинска поговорка). Од кражба на податоци и финансиски малверзации по електронски пат, до оневозможување на услуги, шпионажа, загрозување на критичната инфраструктура и директен напад на нуклеарна програма - дијапазонот е навистина широк. Токму затоа е многу тешко да се дадат конкретни и специфични правни одговори, кои би ги задоволиле барањата на различните предизвици. Структурата на сајбер просторот, а посебно природата на интернетот е спротивна на потребата да биде контролирана. Првото клучно правно прашање би било: чија е јурисдикцијата? Одговорот на тоа прашање во себе ги крие одговорите за правната рамка и импликациите за акција. Но како би можел сајбер просторот да потпадне под чија било јурисдикција? Евентуално може да се зборува за јуридикција врз инфраструктурата која го овозможува постоењето на сајбер просторот, но во суштина, тој не е фиксна категорија. Светот составен од битови и бајтови, не може да се измери, лоцира и алоцира во класичното значење на поимите. Од друга страна, сајбер просторот е место каде што најмногу „се кршат копјата“ во судир помеѓу барањата за безбедност и приватност, а човековите права концептуално се на удар. Во отсутство на консензуален правен одговор, останува да се постигне максимална апликабилност на постоечките правни режими во зависност од конкретната ситуација, односно да се врши посебна анализа за поедничените случаи. Дополнително од различните фактички ситуации кои бараат различни апликабилни правни режими треба да се земат предвид различните пристапи кон сајбер културата и културниот релативитет како таков, зависноста на едно конкретно

[4] Достапно на http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

општество од сајбер просторот, неговата резилиентност кон заканите, намерата на потенцијалните напаѓачи, како и ефектите и последиците измерени во конкретна штета од евентуален напад. Вокабуларот кој се употребува во овој домен, исто така, не е унифициран, што остава дополнителен простор за толкување. Најчесто употребуваните може да се класифицираат во неколку категории:

а) Сајбер напад, термин кој покрива широк спектар на активности со различен карактер и цел, дури и активности кои би можеле да го активираат членот 5 од Договорот од Вашингтон, односно да испровоцираат воен одговор во смисла на колективна самоодбрана на земјите членки на НАТО.[5]

б) Сајбер криминал (crime), познат и под називот електронски криминал, компјутерски криминал и слично, кој опфаќа криминални активности спроведени со користење на компјутери и интернет, најчесто финансиски мотивирани. Компјутерскиот криминал вклучува кражба на идентитет и измама, меѓу другите активности. Компјутерскиот криминал се разликува од другите форми на малициозни сајбер активности, кои имаат политички, воени или мотиви на шпионажа. [6];

в) Сајбер војна (war) или „наменска употреба на компјутерски системи со цел да се прекинат активностите на непријателска земја или напад на нејзините комуникациски системи“[7]. За да се утврди состојба на сајбер војна, мора да има атрибуција (припишливост) на дејствијата кон владини агенти или државни органи. Авторката е на мнение дека токму докажувањето на атрибуцијата најчесто е главен „виновник“ што светот не е барем официјално и во сајбер војна.

г) Сајбер војување (warfare) претставува хибриден термин кој има за цел да опфати поширок спектар на агресивни дејствија. За разлика од војната или кривичните дела, терминот „војување“ не претставува правна категорија. Токму затоа и е често употребуван - опфаќа поширок спектар на дејствија, особено во контекст на современите хибридни и асиметрични безбедносни закани, кои често се наоаѓаат во меѓупросторот на криминалот и војната. Контекстот во кој се употребува најчесто вклучува држава или сојуз на држави како субјект и како барем

5) Достапно на http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/

6) Достапно на https://www.newamerica.org/cyber-global/compilation-of-existing-cybersecurity-and-information-security-related-definitions/

7) Достапно на https://www.newamerica.org/cyber-global/compilation-of-existing-cybersecurity-and-information-security-related-definitions/

една страна. Иако поограничен, како синоним се употребува и терминот електронско војување, кој Талинскиот прирачник го дефинира како „Употреба на електромагнетните полиња (ЕМ) или насочена енергија за искористување на електромагнетниот спектар. Тоа може да вклучува пресретнување или идентификација на емисиите, вклучување на енергија, спречување на непријателската употреба на ЕМ спектар од една спротивна страна, како и активности за да се обезбеди ефикасно вклучување на ЕМ спектар од страна на државата корисник“.

д) Сајбер тероризам - термин кој се употребува за да се посочи на акти на тероризам во сајбер просторот, но и искористување на сајбер просторот како алатка за вршење на дела на тероризам. Може да потпадне под која било од погоре наведените категории во зависност од специфичностите на поединечните околности.

3. Правна рамка за сајбер безбедноста

Сајбер безбедноста е сè повеќе топ тема во светот, а доктината и таканаречената „меко право“ се движат, иако многу полека во насока на изнаоѓање на консензуални решенија и кристализирање на минимум правна рамка.

Во секој случај, може да се зборува за условно кажано две правни рамки: националната како примарна и потесна и меѓународната како поопшта и поширока.

4. Национална правна рамка

Кога станува збор за националната правна рамка во Република Македонија сајбер безбедноста се третира, пред сè, во доменот на сајбер криминалот, во потесна смисла, односно се сведува на класичните дела на компјутерски криминал или употребата на компјутерски системи и мрежи за вршење на дела од „класичниот“ криминал – (компјутерска) измама, (компјутерски) фалсификат, кражба (на лични податоци) и слично, односно националната правна рамка се движи примарно низ материјалното казнено право - Кривичниот законик. Со кривичниот законик се инкриминирани:

а) Член 144, став 4 – Загрозување на сигурноста

„Тој што по пат на информатички систем ќе се закани дека ќе стори кривично дело за кое е пропишана казна затвор од пет години или потешка казна против некое лице поради неговата припадност кон определена национална, етничка или расна група или верска определба, ќе се казни со казна затвор од една до пет години“.

б) Член 147 - Повреда на тајноста на писмата или други пратки.

в) Член 149 – Злоупотреба на лични податоци.

(....Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година. Со казна од став 1 се казнува тој што ќе навлезе во компјутерски Информатички систем на лични податоци со намера користејќи ги за себе или за друг да осгвари некаква корист или на друг да му нанесе некаква штета.)

Казнив е и обидот.

г) Член 149-а – Спречување на пристап кон јавен информатички систем.
д) Член 157 – Повреда на авторско право и сродни права.
ѓ) Член 157-а - Повреда на правото на дистрибутерот на технички посебно заштитен сателитски сигнал.
е) Член 157-б – Пиратерија на аудиовизуелно дело.
ж) Член 157-в – Пиратерија на фонограм.
з) Член 193 – Покажување на порнографски материјал надете.
ѕ) Член 193-Производство и диструбуција на детска порнографија; Намамување на обљуба или друго полово дејствие на малолетник кој не наполнил 14 години.
и) Член 251 - Оштетување или неовластено навлегување во компјутерски систем.
ј) Член 251- Правење и внесување на компјутерски вируси; Компјутерска измама.
к) Член 271 – Правење, набавување или отуѓување средства за фалсификување.
л) Член 274-б - Изработка и употреба на лажна платежна картичка.
љ) Член 279-а - Компјутерски фалсификат.
м) Член 286 - Повреда на правото од пријавен или заштитен пронајдок и топографија на интегрални кола.
н) Член 394-г - Ширење на расистички и ксенофобичен материјал по пат на компјутерски систем.

Покрај Кривичниот законик, релевантни се и Законот за кривична постапка кој се однесува на процесните норми воопшто, а кои подеднакво важат и за процесуирање на делата поврзани со сајбер криминал кои ги инкриминира кривичниот законик. Посебни одредби од ЗКП има за пребарување на компјутерски систем и компјутерски податоци (член 184) и привремено одземање на компјутерски податоци (член 198), а делумно и во делот кој се однесува на мерки за пронаоѓање и обезбедување на лица

и предмети, како и во делот за посебните истражни мерки (таен увид и пребарување во компјутерски систем и увид во остварени телефонски и други електронски комуникации).

Дополнително, определени сегменти се опфатени и со:

– Законот за електронските комуникации;
– Законот за следење на комуникациите;
– Законот за електронска трговија;
– Законот за електронско управување (е-влада);
– Законот за податоците во електронски облик и електронски потпис.

Република Македонија е членка на Конвенцијата за сајбер криминал[8] на Советот на Европа. Со тоа што Конвенцијата е ратификувана, станува дел од внатрешниот правен поредок согласно со Уставот на Р. Македонија[9].

5. Конвенцијата за сајбер криминал на Совет на Европа

Конвенцијата за сајбер криминал (односно Конвенцијата за компјутерски криминал, согласно Законот за ратификација на истата во Р. Македонија) е првиот меѓународен договор кој третира кривични дела извршени преку интернет и други компјутерски мрежи, кои се занимаваат особено со прекршувањата на авторските права, компјутерска измама, детска порнографија и нарушување на мрежна безбедност. Таа, исто така, содржи серија на овластувања и процедури, како што се пребарување на компјутерски мрежи и пресретнување. Нејзината главна цел, во духот на преамбулата е да се продолжи со заедничка политика во насока на заштита на општеството од компјутерскиот криминал, особено преку усвојување на соодветно законодавство и поттикнување на меѓународната соработка.

Истата во себе содржи материјални и процесни аспекти, во насока на хармонизирање на законодавството помеѓу земјите членки на истата.

Конвенцијата е воедно најзначајниот меѓународен правен акт во областа. Иако постојат и други регионални иницијативи и документи, истата важи за најконкретна и најсеопфатна досега. Иницијативите одат дотаму што неодамна беше предложен и нацрт-документ со кој би се воспоставил меѓународен трибунал за сајбер злосторства, но во принцип квантитаивно гледано, бројот на иницијативите е далеку поголем од реализираните проекти или конкретните ефекти[10].

---

8) Достапно на http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

9) Достапно на http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=efXr75F0

10) Види повеќе на http://www.cybercrimelaw.net/documents/Draft_Treaty_text_on_

Во принцип и националната правна рамка и Конвенцијата на Советот на Европа се движат во делот на компјутескиот криминал и базичните дела.

6. Меѓународно-правни аспекти на сајбер безбедноста

Во поглед на сајбер војувањето и сајбер војните, епски потфат е изготвувањето на Талинскиот прирачник за меѓународно право апликабилно при сајбер војување ("Tallinn Manual on the International Law Applicable to Cyber Warfare") изготвен од група на експерти, со намера да обезбеди одговори и кодификација[11]. Во принцип, се сведува на поделба на режимите и апликабилност на jus ad bellum и jus in bello, односно на „правото да се оди во војна" и правото кое е апликабилно во војна, навраќајќи се на општите принципи на меѓународното право. Ако од ова се тргнува, вреди да се спомене пресудата на Меѓународниот суд на правдата, судски орган на Обединетите нации, во случајот помеѓу Никарагва и Соединетите Американски Држави[12], во која меѓудругото се вели дека индивидуална или колективна самоодбрана државата може да употреби само против „вооружен напад", а за да се констатира постоење на истиот, се земаат предвид „опсегот и ефектите" на истиот. Иако и оваа судска пресуда вклучува вооружени сили, што е донекаде на линија со Женевските конвенции, остава многу поширок простор за толкување.

Во отсуство на прецизна правна рамка и реално тешко постиглив консензус околу истата, клучните актери се фокусираат многу повеќе на развој на „политики" (policy) како modus operandi за делување и реакција. Зголемена посветеност на политиката може да се види во завршните согледувања од самитот во Букурешт во 2008 година, во која НАТО членките ги истакнаа своите заложби за усвојување на политики за сајбер одбрана, во смисла на „потреба на НАТО и земјите да ги заштитат клучните информациски системи; да споделат најдобри практики; и за да се обезбеди способност да им помогне на земјите сојузнички, на барање, да се спротивстават на сајбер напад[13]". НАТО ја постави сајбер одбраната како клучен приоритет во својот нов стратешки концепт од 2010[14]

International_Criminal_Tribunal_for_Cyberspace.pdf

11) Прирачникот е достапен на https://ccdcoe.org/tallinn-manual.html

12) Целиот текст е достапен на http://www.icj-cij.org/docket/?sum=367&p1=3&p2=3&case=70&p3=5

13) NATO, Bucharest Summit Declaration para. 47 (Apr. 3, 2008).

14) NATO, Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, (Nov. 2010), достапно на

и продложи со континуираните залагања за интегрална сајбер одбрана[15].

Ваквиот пристап може да делува како конфузен и нецелесообразен на прв поглед, но тоа е така заради структурата и поставеноста на меѓународното право како такво. Имено, за извори на меѓународното право согласно со Статутот на Меѓународниот суд на правдата со седиште во Хаг, Холандија, кој е главен судски орган на ООН се земаат предвид:

- меѓународните договори (договорно право);
- меѓународно воспоставениот обичај (обичајно право, односно континуирана практика на државите проследена со opinion iuris или свест за таквата практика);
- општи принципи на правото признаени од цивилизираните народи;
- судските одлуки;
- мислењата на истакнатите правници, со тоа што последните два извори претставуваат дополнителен извор на правото и кон него се „прибегнува“ за генерирање односно создавање на меѓународно-правни правила, како и за помошно толкување.

Во овој дел, на сајбер просторот му недостигаат кохерентни и договорни и обичајни правни правила. Креирањето на мултилатерални договори согласно со Виенската конвенција за договорно право е сложен процес, но пред сè клучниот проблем лежи во специфичноста на сајбер просторот и неподобноста за негово регулирање, како и физичките тешкотии - во смисла на сопственост врз инфраструктурата, на пример.

Но, постои определена правна рамка за определени аспекти или состојби. На пример, Меѓународната телекомуникациска унија[16], има свои правила и прописи за определени сегменти кои потпаѓаат под сајбер безбедноста.

Професорот Курбалија, пак, смета дека иако не постои специфичен режим за регулирање на она што тој го квалификува како „internet governance“, постои широк спектар на правни инструменти кои може да се аплицираат[17]. Тука ја наведува судската практика на САД кои имаат најбогато искуство во овој дел, како и општите правила за установување на јурисдикција, документите кои произлегуваат од Светскиот самит на

http://www.nato.int/nato_static/assets/pdf/pdf_publications/ 20120214_strategic-concept-2010-eng.p

15) Достапно на http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf

16) Види повеќе на http://www.itu.int/en/Pages/default.aspx

17) Kurbalija, J. Internet Governance 6th edition

информатичко општество, арбитражата како механизам и слично. Сепак, ова е далеку од доволно за да се постигне ефективна и интегрирана сајбер безбедност, по мнение на авторката.

Заклучок

Справувањето со безбедносните сајбер закани бара специфицирани знаења и мултидисциплинарен пристап. Правната рамка не е кохерентна, ниту пак со оглед на постојаниот напредок е возможно да се постигне конечен и унифициран правен одговор. Уште потешки се практичните импликации и обидот да се спроведе доследно истата.

Заканите и понатаму ќе растат и ќе мутираат. Ефективната заштита лежи во превенцијата и зајакнувањето на информатичкото општество- и во тоа правната рамка токму во тој сегмент да зајакне. Тоа подразбира подготовка на стратегија за сајбер безбедност, со воспастувавање на целата институционална рамка која од неа произлегува, како и ефектуирање на фискалните импликации. И најдоброто законско решение не може да биде ефективно без механизам за имплементација и без за него да се предвидаат соодветни фискални импликации.

Градењето на партнерставата е неопходно, но истото треба да е базирано на стратешки институционален пристап, опфаќајќи ги академската и бизнис заедницата, владините институции и цивилното општество, со визија за изградба на резилиентно општество базирано на едукација и кибернетска култура.

Излезот во секој случај ќе се бара во најдобрите пракитки и идејата за саморегулирање, барем уште извесно време.

БИБЛИОГРАФИЈА

CCDCOE (2013) The Tallinn Manual, достапно на http://www.ccdcoe.org/tallinn-manual.html

Kurbalija, J. Internet Governance 6th edition.

NATO, Bucharest Summit Declaration (2008).

NATO, Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization (2010).

Законот за електронските комуникации на РМ.

Законот за следење на комуникациите на РМ.

Законот за електронска трговија на РМ.

Законот за електронско управување (е-влада) на РМ.

Законот за податоците во електронски облик и електронски на РМ.

Кривичен закон на РМ.
Закон за кривична постапка на РМ.
Конвенција за компјутерски криминал на Совет на Европа.
Статут на Меѓународен суд на правдата (МСП).
Советодавно мислење на МСП во случајот Палестинки sид.
Пресуда на МСП во случајот на Никарагва против САД.