Министарство одбране
Универзитет одбране
Институт за стратегијска истраживања

ХИБРИДНО РАТОВАЊЕ

дилема концепта савремених сукоба

Тематски зборник

Београд
2018

Хибридно ратовање

–

дилема концепта савремених сукоба

Тематски зборник радова

Београд, 2018

Издавач

Институт за стратегијска истраживања
Универзитет одбране
Република Србија

За издавача

др Јованка Шарановић, научни сарадник

Уредник

пуковник др Небојша Николић, научни сарадник

Рецезенти

др Дарко Трифуновић, виши научни сарадник
др Станислав Стојановић, научни сарадник

Дизајн
пуковник др Мирослав Митровић

Технички уредник
потпуковник МА Милинко Врачар

ISBN 978-86-81121-21-4

САДРЖАЈ

СТРАТЕШКЕ КОМУНИКАЦИЈЕ И САЈБЕР ПРОСТОР КАО ПОПРИШТА ХИБРИДНОГ РАТОВАЊА

ИНДИКАТОРИ САЈБЕР ПРЕТЊИ: АНАЛИЗА ИНДЕКСА ГЛОБАЛНЕ САЈБЕР БЕЗБЕДНОСТИ

Иван Р. Димитријевић*,
Факултет безбедности, Универзитет у Београду

Ана Параушић**
Факултета безбедност, Универзитет у Београду

Апстракт: Значај мрежа, уређаја и услуга у области информационих и комуникационих технологија (ИКТ) данас је очигледан и пресудан за нормално функционисање скоро свих држава света. Око пола светског становништва користило је интернет у 2016. години, а процењује се да ће до 2020. године 12 милијарди уређаја бити повезано на интернет, директно или преко других уређаја. Јасно је да постоји узрочно-последична веза између раста информационих и комуникационих технологија и њихове незаконите и злонамерне употребе. Због тога скоро све државе света развијају стратегије за подизање нивоа своје сајбер безбедности. Међутим, и даље постоје велике разлике међу државама у погледу свести, разумевања, знања и капацитета за спровођење адекватних стратегија и програма како би се осигурала безбедна и одговарајућа употреба ИКТ као покретача економског развоја држава.

Због тога је Међународна унија за телекомуникације (International Telecommunication Union, ITU), заједно са међународним партнерима из јавно-приватног и приватног сектора, као и из академске заједнице, израдила Индекс глобалне сајбер безбедности (Global Cybersecurity Index, GCI). Кључни циљ Индекса глобалне сајбер безбедности јесте изградња капацитета на националном, регионалном и међународном нивоу кроз процену степена ангажовања држава око сајбер безбедности, као и израда листе примера добре праксе која се може користити у државама којима је потребна помоћ у овој области.

Индекс је покренут 2014. године кад је спроведено прво истраживање међу државама чланицама ITU (GCI 2014), и он се заснива на тзв. пет стубова који чине Глобалну агенду за сајбер безбедност (Global Cybersecurity Agenda, GCA). У анализи ћемо користити податке и извештаје Међународне уније за телекомуникације (ITU), односно поред Индекса глобалне сајбер безбедности 2014 и Индекса глобалне сајбер безбедности 2017, анализираћемо и одабране појединачне профиле сајбер безбедности држава чланица ITU из Европе, са посебним фокусом на Републици Србији. Анализираћемо које претње су препознате у области сајбер безбедности и на које начине су државе света спремне за суочавање са овим претњама.

* ivan.dimitrijevic@fb.bg.ac.rs
** parausicana@gmail.com

Кључне речи: сајбер претње, сајбер безбедност, Индекс глобалне сајбер безбедности.

УВОД

Развојем информационих и комуникационих технологија (ИКТ) с почетка 21. века, појавио се читав спектар безбедносних изазова, ризика и претњи по овај кључни ресурс. Информационе и (теле)комуникационе мреже данас представљају стуб функционисања практично свих држава света, а о комплексности ових технологија најбоље говори чињеница да оне више нису део изолованих домена, као што су приватни, државни и међународни, већ су сплет њихове међузависности. С друге стране, „развој информационих и комуникационих технологија омогућио је потенцијалним носиоцима асиметричних претњи да увећају своје капацитете за напад на традиционалне субјекте националне безбедности" (Dimitrijević & Stekić, 2018:653). Управо овај аспект утицао је на то да се претње у овој области схвате много озбиљније на почетку 21. века кад се појављују први конкретни сајбер напади у контексту савремених сукоба ниског интензитета у литератури и јавном дискурсу познатих као „хибридно ратовање".

У извештају Војни биланс (*Military Balance*) за 2015. годину Међународног института за стратегијске студије (*International Institute for Strategic Studies*), „хибридно ратовање" одређено је као „употреба војних и невојних средстава у интегрисаној кампањи усмереној на изазивање изненађења, преузимање иницијативе и стицање психолошке и физичке предности кроз употребу дипломатских средстава; *софистицираних и брзих информационих, електронских и сајбер операција*;[1] прикривених и у неким случајевима отворених војних и обавештајних активности; и економских притисака" (IISS, 2015:5). На сличан начин се и у јавном дискурсу одређује овај појам, као „стапање дипломатије, политике, медија, *сајбер простора*[2] и војне силе ради дестабилизације и подривања противничких влада" (Standish, 2018).

У западној литератури доминира приступ да је „хибридно ратовање", поред тога да је у питању „комбинација конвенционалног и иррегуларног ратовања", своју садашњу форму достигло руском анексијом Крима, а да је касније настало као резултат неколико случајева убацивања малициозних софтвера у информационе системе критичних инфраструктура и државних институција од стране Руске Федерације. У руској литератури и у јавном дискурсу, пак, појам „хибридног ратовања" везује за широк спектар пропагандних и других невојних активности које спроводе западне државе предвођене Сједињеним Америчким Државама. Без обзира на размимоилажења у политичким предзнацима ових приступа, „хибридно ратовање" можемо посматрати као „заобилазни" пут у савременом политичком, економском и војном надметању великих сила, где засигурно доминирају средства која максимално експлоатишу убрзани развој информационих и комуникационих технологија.

[1] Курзив аутора текста.
[2] Исто.

Управо из овог разлога, оно што током последње деценије у литератури доминира као претња из домена „хибридног ратовања“, то су разноврсне сајбер претње, односно безбедносне претње које државни и недржавни актери усмеравају на информационе, комуникационе и друге системе критичне инфраструктуре и објекте од значаја по националну безбедност, држава које су означене као мете напада. Поред различитих начина изградње капацитета за одбрану од сајбер претњи, државе у сарадњи са приватним компанијама и међународним организацијама развијају и одређене глобалне стандарде који треба да буду успостављени како би се умањиле последице ових претњи и како би се олакшало реаговање на њих, посебно уколико је сајбер нападима обухваћено више држава. Ово је важно јер „функционалне, развијене и добро организоване државе које објективно разматрају изазове, ризике и претње и укључују неопходне ресурсе за њихово елиминисање или спречавање, имају реалне шансе да постану потенцијално тежак и захтеван објекат могућих хибридних операција“ (Mitrović, 2017:329).

Због свега наведеног, покренут је Индекс глобалне сајбер безбедности (*Global Cybersecurity Index, GCI*), који представља иницијативу великог броја државних и недржавних актера која је првенствено усмерена на мерење посвећености држава повећању сајбер безбедности на националном, регионалном и међународном нивоу. Да бисмо разумели предмет који се налази у центру истраживања и квантитативног исказивања овог Индекса, потребно је укратко одредити појам сајбер безбедности. Сајбер безбедност „комбинује карактеристике 'јавних добара' које се често повезују са одговорношћу држава, са широким спектром добара и услуга на приватном тржишту, а истовремено обухвата умрежене форме организације које укључују нетржишне и недржавне ресурсе, као и размену информација“ (Kuerbis, Badiei, 2017:1). У литератури се често прави разлика између појмова „информациона безбедност“ и „сајбер безбедност“. Тако, Пенг сматра да се информациона безбедност односи на заштиту права на приватност, док је сајбер безбедност питање од значаја за националну безбедност: „У оквирима суштине регулисања, иако оба концепта имају за циљ остваривање безбедносних карактеристика поверљивости и интегритета, питања сајбер безбедности усмерена су на очување функционисања критичних инфраструктура, док информациона безбедност тежи спречавању откривања личних података“ (Peng, 2015:21).[3] Управо у том контексту, ITU препоручује да се сајбер безбедност посматра као питање националне политике, пре свега због тога што би злоупотреба сајбер простора могла негативно да утиче на економско добростање, јавно здравље и националну безбедност (ITU, 2015).

ИНДЕКС ГЛОБАЛНЕ САЈБЕР БЕЗБЕДНОСТИ (GCI)

Међународна унија за телекомуникације (*International Telecommunication Union, ITU*), заједно са међународним партнерима из јавно-приватног и приватног сектора, као и из академске заједнице, покренула је Индекс глобалне

[3] У Републици Србији се појам информационе безбедности користи и у контексту сајбер безбедности, те ову област регулише Закон о *информационој безбедности*, а тело надлежно за питања сајбер безбедности се зове Тело за координацију послова *информационе безбедности*, те се у том смислу ова два израза могу користити и као синоними.

сајбер безбедности (*Global Cybersecurity Index, GCI*). Кључни циљ Индекса глобалне сајбер безбедности јесте изградња капацитета на националном, регионалном и међународном нивоу кроз процену степена ангажовања држава око сајбер безбедности, као и израда листе примера добре праксе која се може користити у државама којима је потребна помоћ у овој области. Разлог за мерење Индекса лежи у чињеници да се претње по рачунарске мреже више не могу игнорисати због пораста броја малициозних софтвера и повећања напада на пословање и кориснике услуга, док актери који данас спроводе ове нападе имају политичке, криминалне, терористичке или хакерске мотиве.

Индекс је покренут 2014. године кад је спроведено прво истраживање међу државама чланицама ITU (GCI 2014), с циљем да се „...пружи тренутна слика стања о томе где се налазе државе чланице кад је у питању посвећеност сајбер безбедности на националном нивоу. Замисао иза овог циља лежи у промовисању свести о сајбер безбедности, као и значаја улоге званичних власти у интегрисању одговарајућих механизама за подршку и промовисање сајбер безбедности" (GCI, 2015). Индекс из 2014. године обухватио је примарно и секундарно истраживање. Све државе чланице ITU добиле су упитнике који су допуњавани дубинским квалитативним истраживањем, а истраживање је подразумевало прикупљање података и информација о законском оквиру, регулативи, CERT-овима и CIRT-овима, званично прокламованим политикама у области сајбер безбедности и усвојеним стратегијама, стандардима и сертификацији, професионалном оспособљавању, подизању свести и партнерствима у овој области (GCI, 2015).

Тренутно је у оптицају друга верзија Индекса (GCI 2017), и он се заснива на тзв. *пет стубова* који чине Глобалну агенду за сајбер безбедност (*Global Cybersecurity Agenda, GCA*): 1) *законски* (да ли постоји правни основ?); 2) *технички* (да ли постоје техничка тела и оквири?); 3) *организациони* (да ли постоје институције за координацију политике и развој стратегија за сајбер безбедност на националном нивоу?); 4) *изградња капацитета* (да ли постоје програми истраживања и развоја, обуке и едукације?); и 5) *сарадња* (да ли постоје партнерства, оквири за сарадњу и мреже за размену информација?). Сваки од стубова садржи поткатегорије, односно индикаторе који се мере у процесу прикупљања података о државама чланицама:

- *I стуб*: законодавство у области сајбер криминала, регулатива у области сајбер безбедности, обука у области сајбер безбедности;
- *II стуб*: национални CERT, владин CERT, секторски CERT-ови, стандарди за организације, стандарди и сертификација за професионалце, онлајн заштита деце;
- *III стуб*: стратегија, одговорно тело/институција, мерење сајбер безбедности;
- *IV стуб*: тела за стандардизацију, добре праксе, програми истраживања и развоја, кампање за подизање јавне свести, курсеви за професионалну обуку, национални образовни програми и академски програми, механизми за покретање иницијатива, самостална индустрија сајбер безбедности;
- *V стуб*: унутардржавна сарадња, мултилатерални споразуми, учешће у међународним форумима, јавно-приватно партнерство, партнерство између различитих агенција.

Индекс глобалне сајбер безбедности стога садржи укупно 25 индикатора и 157 одговарајућих питања. Индикатори за израчунавање GCI бирани су на основу следећег сета критеријума:

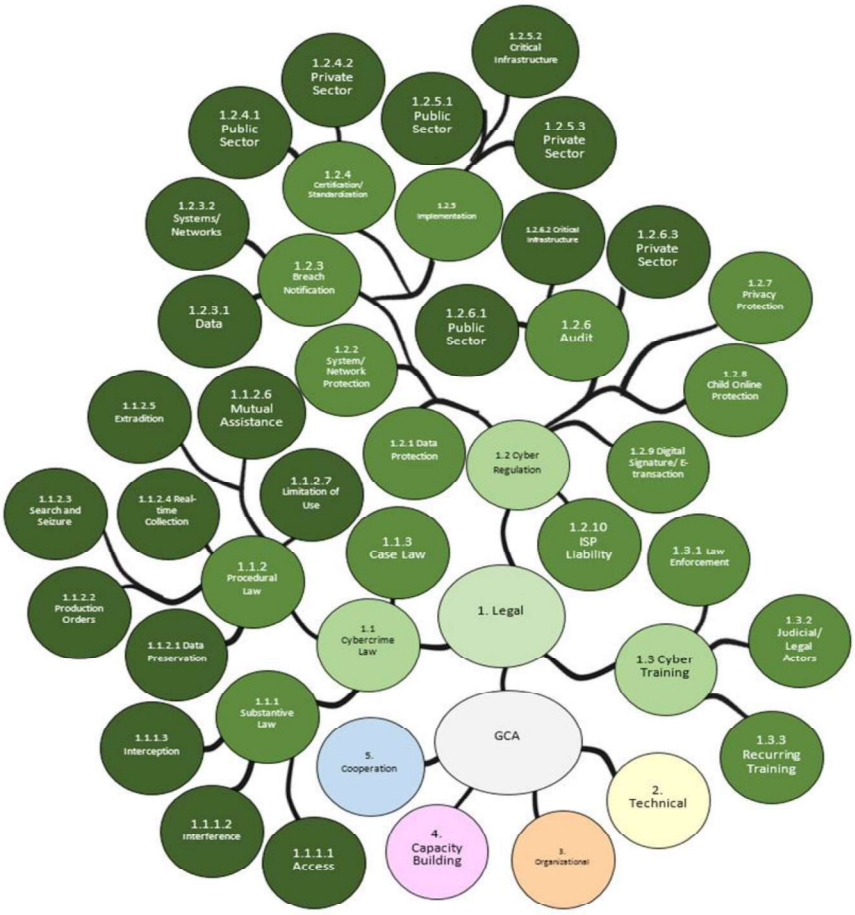
- значаја за пет GCA стубова и доприноса главним циљевима GCI и његовом концептуалном оквиру;
- доступности и квалитета података;
- могућности верификације путем секундарних података (ITU, 2017:9).

Целокупни концепт нове верзије GCI заснован је на тзв. *tree map*[4] визуелизацији развоја сајбер безбедности и на пружању бинарних одговора (ITU, 2017:9). Концепт *tree map* визуелизације представља пример различитих могућих приступа које државе могу предузети како би оснажиле своју сајбер безбедност. Сваки од пет стубова приказан је одређеном бојом. Што је развијенији конкретни приступ, а то истовремено указује и на већи ниво посвећености у тој области, то је тамнија боја којом се овај приступ илуструје (ITU, 2017:9), што се може видети на слици 1.

Размотрени су различити нивои развоја сајбер безбедности међу земљама, као и различите потребе сајбер безбедности, које се огледају у укупном стању развијености ИКТ. Концепт се заснива на претпоставци да што је развијенија сајбер безбедност, то ће комплекснија решења бити уочена. Због тога, што даље конкретна држава прође кроз *tree map* структуру, чиме потврђује присуство унапред дефинисаних сајбер решења, то ће сложенија и софистицираније бити њена обавеза према сајбер безбедности, и то јој омогућава да добије виши GCI скор (ITU, 2017:9).

Разлог за употребу могућности бинарних одговора на дата питања лежи у елиминацији процене засноване на ставовима и евентуалне пристрасности према одређеним врстама одговора (ITU, 2017:9). Штавише, једноставни бинарни концепт ће омогућити бржу и сложенију евалуацију јер неће захтевати опширне одговоре из појединачних држава. Ово, заузврат, може убрзати и усмеравати процес давања одговора и даље евалуације. Идеја је да ће испитаник само потврдити присуство или одсуство одређених унапред идентификованих решења у области сајбер безбедности. Механизам онлајн анкета, који се користио за прикупљање одговора и преношење свих релевантних материјала, омогућио је креирање добре праксе (ITU, 2017:9).

[4] У питању је визуелизација хијерархијских структура информација која се представља у виду стабла, односно разгранате структуре.



Слика 1. Tree map визуелизација на примеру I (законског) стуба.
Стабло илуструје однос између GCA, остала четири стуба,
индикатора и конкретних питања.
Извор: (GCI 2017:7)

Кључна разлика у методологији између GCI 2014 и GCI 2017 је коришћење бинарног система уместо тростепеног система. Помоћу бинарног система процењује се постојање или одсуство одређене активности, одељења или мере. За разлику од верзије GCI из 2014. године, у верзији из 2017. године не узимају се у обзир „парцијалне" мере. Могућност да испитаници пошаљу пратећу документацију и УРЛ-ове јесте начин да се пруже детаљније информације како би се поткрепили бинарни одговори. Надаље, у сваком од пет стубова је додато више нових питања како би се побољшала дубина истраживања (ITU, 2017:9). GCI из 2014. године и GCI из 2017. године нису потпуно упоредиви услед промена у методологији прикупљања података. Док је у Индексу из 2014. године коришћена једноставна метода средње вредности, у креирању Индекса за 2017. годину коришћени су тежински фактори за сваки стуб (ITU, 2017:9).

Табела 1. Број одговора добијених од држава чланица
по регионима (ITU, 2017:10)

Регион	**Африка**	**Америка**	**Арапске државе**	**Азија и Пацифик**	**Заједница нез. држава**	**Европа**	**Глобално**
Попуњени упитници	29	23	16	25	7	34	134
Непопуњени упитници	15	12	5	13	5	9	59
Укупан број учесника	44	35	21	38	12	43	193

Упитник, који је био доступан онлајн од јануара до септембра 2016. године, послат је у 193 државе чланице Међународне уније за телекомуникације (плус Палестина) у регионима Африке, Америке, арапских држава, Азије и Пацифика, Заједнице независних држава и Европе. Упитник су попуниле 134 земље, док 59 земаља није доставило попуњене упитнике (табела 1) (ITU, 2017:9).

Кад је у питању методологија израде Индекса глобалне сајбер безбедности 2017, сам процес прикупљања података састојао се из неколико корака:

1. **Позивно писмо** послато је свим држава чланицама посредством Секретаријата Међународне уније за телекомуникације, у којем су обавештене о покренутој иницијативи и замољене да предложе лице одговорно за GCI с којим би ITU комуницирала и које би било одговорно за прикупљање свих релевантних података за попуњавање онлајн упитника. Заједно са позивним писмом послато је и упутство за попуњавање упитника у коме су се налазила појашњења и илустративни примери за свако питање.[5]

2. **Прикупљање примарних података** (за државе које су послале попуњене упитнике) (ITU, 2017:10):

- Провера одговора добијених од држава чланица ради идентификације потенцијално недостајућих елемената (нема одговора, нема пратећих докумената, нема хиперлинкова итд.).
    - На пример, ако је држава чланица на неко питање одговорила са "НЕ", ITU је обавила претрагу како би се утврдило да ли постоје било какава документа у бази података ITU или онлајн.

[5] Упутство је доступно на званичној интернет презентацији Међународне уније за телекомуникације: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide -E.pdf.

- Ако је држава чланица на неко питање одговорила са "ДА", ITU је обавила претрагу како би проверила да ли су одговори тачни и кореспондирају са питањем.

- Контакт особа која је одређена од конкретне државе чланице контактирана је и добила је упутства о томе како побољшати прецизност одговора. Уколико је то потребно, ITU је дала коментаре и упутства за побољшање попуњеног упитника.
- После неопходних кругова понављања, прелиминарна верзија попуњеног упитника је упућена назад држави чланици на коначно одобрење.
- Кад је примљена формална сагласност, упитник се сматра ваљаним и користи се за анализу, оцењивање и рангирање.

3. **Прикупљање секундарних података** (за државе које нису доставиле попуњене упитнике) (ITU, 2017:10-11):

- ITU је разрадила почетни нацрт одговора на упитник користећи јавно доступне податке и онлајн истраживања.
- Нацрт је затим упућен конкретној држави чланици на разматрање.
- Након редиговања одговора, контакт особа која је идентификована од стране државе чланице, контактирана је и добила упутства о томе како побољшати прецизност одговора. Уколико је то потребно, ITU је дала коментаре и упутства за побољшање попуњеног упитника.
- После неопходних кругова понављања, прелиминарна верзија попуњеног упитника је упућена назад држави чланици на коначно одобрење.
- Кад је примљена формална сагласност, упитник се сматра ваљаним и користи се за анализу, оцењивање и рангирање. Стратегија рангирања названа је „густо рангирање“ (dense ranking), при чему државе чланице са једнаким GCI скором добијају исти редни број, а следећа земља добија наредни редни број, чиме се одражава рангирање према GCI скору.6

КЉУЧНИ НАЛАЗИ ИНДЕКСА ГЛОБАЛНЕ САЈБЕР БЕЗБЕДНОСТИ 2017

Најмање једна држава из сваког од шест региона ITU налази се у првих десет места у Индексу 2017 (табела 2). Три су из Азије и Пацифика, по две из Европе и Америке, и по једна из Африке, арапских држава и Заједнице независних држава, што иде у прилог тврдњи да висока посвећеност сајбер безбедности не мора да буде повезана са географском локацијом. Постоји значајан јаз када је у питању сајбер приправност *(Cyber Preparedness)* широм света, како између различитих ITU региона, тако и унутар самих региона (ITU, 2017:17).

[6] Развој методологије GCI за 2017. годину подразумевао је и консултовање стручњака, идентификованих према њиховој специфичној области стручности, како би пружио и експертски поглед на начин бодовања (ITU, 2017:11).

Обавезе држава према сајбер безбедности често су неуједначене пошто постоје државе које остварују добре резултате у неким стубовима, а слабије у другим. Према ITU, „сајбер безбедност је екосистем у којем закони, организације, вештине, сарадња и техничка имплементација морају бити у хармонији како би били најефикаснији“ (ITU, 2017:17). Поред тога, сајбер безбедност није само обавеза националних влада, већ захтева и подједнаку посвећеност приватног сектора и корисника услуга. Стога је важно развити културу сајбер безбедности где су грађани свесни компромиса између ризика и надзора током коришћења електронских мрежа (ITU, 2017:17).

Табела 2. Првих десет држава према скоровима GCI 2014 и GCI 2017

GCI 2014		**GCI 2017**	
Држава	**Индекс**	**Држава**	**Скор**
САД	0,824	Сингапур	0,92
Канада	0,794	САД	0,91
Аустралија	0,765	Малезија	0,89
Малезија	0,765	Оман	0,87
Оман	0,765	Естонија	0,84
Нови Зеланд	0,735	Маурицијус	0,82
Норвешка	0,735	Аустралија	0,82
Бразил	0,706	Грузија	0,81
Естонија	0,706	Француска	0,81
Немачка	0,706	Канада	0,81

Као што је већ речено, GCI се састоји од 25 различитих индикатора. Неки се односе на прецизне обавезе које помажу у конкретизацији специфичних активности држава у области сајбер безбедности широм света (ITU, 2017:17), а једна од најважнијих обавеза јесте постојање стратегије сајбер безбедности која треба да опише на које ће се све начине држава припремити и реаговати на сајбер нападе на своје дигиталне мреже. Према Индексу 2017, тренутно само 38% држава чланица има објављену стратегију сајбер безбедности, док још 12% држава чланица ради на креирању стратегије сајбер безбедности (ITU, 2017:17).[7] Такође, у Индексу 2017 наглашено је да је потребно уложити више напора у овој области, посебно кад националне владе дигиталне ризике посматрају као ризике високог приоритета. У области обуке, напори морају бити унапређени посебно оних који ће се највероватније законски обрачунавати са кривичним дела у области сајбер безбедности, с обзиром да мање од половине држава чланица

[7] Више детаља о садржају, обиму и квалитету одабраних стратегија сајбер безбедности у: Shafqat & Masood, 2016. Аутори су анализирали стратегије двадесет држава кроз четири категорије: законске, оперативне, техничке и политичке мере, и упоређивали су резултате истраживања са рангирањем држава чланица у односу на GCI скорове.

(43%) има програме изградње капацитета за спровођење закона и правосудни систем (ITU, 2017:17).

Упркос томе што половина држава чланица нема стратегију сајбер безбедности, 61% држава чланиса има тимове за реаговање у ванредним ситуацијама (CIRT, CSRIT или CERT) на националном нивоу, али тек нешто више од петине држава чланица (21%) објављује статистику инцидената у области сајбер безбедности. Према Индексу 2017, ово отежава објективну процену инцидената за већину земаља и утврђивање да ли мере заштите функционишу (ITU, 2017:18). Нешто мање од трећине земаља (32%) потврдило је постојање домаће индустрије сајбер безбедности, с тим да је потребно уложити много више напора у овој области јер би локална индустрија на тај начин имала много боља знања о околностима на националном нивоу, и тиме учинити безбедан сајбер екосистем одрживим. Потенцијал за глобалну сарадњу већи је због активног учешћа на међународним форумима у области сајбер безбедности. Ово је готово универзално питање, пошто је на њега чак 95% земаља одговорило потврдно (ITU, 2017:18).

ЕВРОПСКЕ ДРЖАВЕ И ПОЛОЖАЈ РЕПУБЛИКЕ СРБИЈЕ У ИНДЕКСУ 2017

У кључним налазима Индекса глобалне сајбер безбедности за 2017. годину каже се да у укупно 193 државе чланице ITU постоји „велики распон у погледу посвећености сајбер безбедности“ (ITU, 2017:13), што су аутори извештаја и илустровали одговарајућом мапом посвећености (слика 2). У односу на GCI скор, државе су груписане у три категорије, односно фазе посвећености сајбер безбедности:

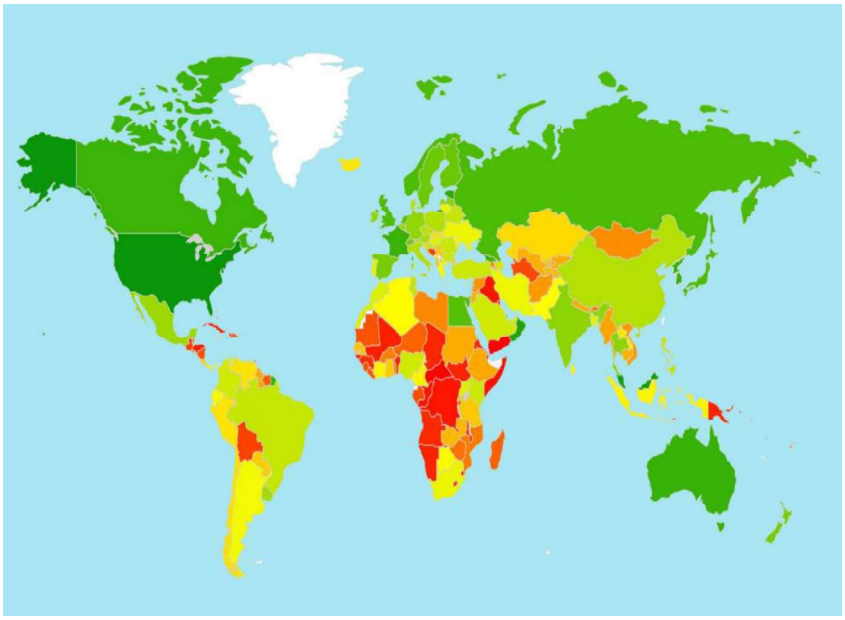
- *Иницијална фаза* (GCI скор налази се испод 50. перцентила), коју чини 96 држава за које би могло да се каже да су започеле са посвећеношћу сајбер безбедности;
- *Фаза сазревања* (GCI скор налази се између 50. и 89. перцентила), коју чини 77 држава које су су развије комплексну посвећеност и укључиле се у програме и иницијативе сајбер безбедности;
- *Фаза лидерства* (GCI скор у 90. перцентилу), коју чини 21 држава које исказују високу посвећеност у свих пет стубова Индекса (2017:13).

Естонија је најбоље рангирана земља у региону Европе. Као и Грузија, Естонија је појачала своју посвећеност сајбер безбедности након сајбер напада 2007. године. Ово је обухватало увођење организационе структуре која може брзо да одговори на нападе, као и усвајање правног оквира према којем се све виталне услуге морају одржавати на минималном нивоу функционисања уколико дође до прекида везе са интернетом. У Естонији се такође налази седиште Здруженог центра НАТО за сајбер одбрану (ITU, 2017:36).

Француска је друга најбоље рангирана земља у региону Европе, и има савршени скор 100 у области изградње капацитета. У земљи постоји широко распрострањена едукација о сајбер безбедности, а Национална агенција за безбедност информационог система објављује листу десетина универзитета акредитованих за дипломе у области сајбер безбедности (ITU, 2017:36).

Норвешка је треће најбоље рангирана земља у Европи, са највишим резултатом у области законодавства. Осим закона који се баве сајбер

безбедношћу, Норвешка је такође спровела истраживање о култури сајбер безбедности, укључујући анкетно испитивање грађана о томе да ли би и у којој мери прихватили праћење њихових онлајн активности (ITU, 2017:36).



Слика 2. Степен посвећености (зелена – највиша, црвена – најнижа)
Извор: (ITU, 2017:13)

Табела 3. Најбоље рангиране земље у Европи

Држава	**GCI скор**	**I**	**II**	**III**	**IV**	**V**
Естонија	0.84	0.99	0.82	0.85	0.94	0.64
Француска	0.81	0.94	0.96	0.6	1	0.61
Норешка	0.78	0.96	0.89	0.64	80.8	0.57

У извештају из 2015. године наводи се да Република Србија има индекс 0,256 и да дели 20. место са још две државе у укупном рангирању сајбер безбедности држава.[8] Према истом извештају, за европски континент Република Србија има индекс 0,2647 и рангирана је на 16. од укупно 22 места (ITU, 2015). У

[8] Глобално рангирање у извештају из 2015. године препознаје укупно 29 група.

извештају из 2017. године наводи се да Република Србија има индекс 0,311 и да се налази на 89. позицији од укупно 164 државе, док је међу европским државама на 37. месту до укупно 43 државе (ITU, 2017). У погледу посвећености сајбер безбедности рангирана је у иницијалној фази, где најбоље скорове показује у другом, техничком и трећем, организационом стубу (видети табелу 4).

Табела 4. Преглед индикатора GCI за Републику Србију
према GCI скору за 2017.

Категорија/Индикатор	**Посвећеност**
Законски	
законодавство у области сајбер криминала	
регулатива у области сајбер безбедности	
обука у области сајбер безбедности	
Технички	
национални CERT	
владин CERT	
секторски CERT-ови	
стандарди за организације	
стандарди и сертификација за професионалце	
онлајн заштита деце	
Организациони	
стратегија	
одговорно тело/институција	
мерење сајбер безбедности	
Изградња капацитета	
тела за стандардизацију	
добре праксе	
програми истраживања и развоја	
кампање за подизање јавне свести	
курсеви за професионалну обуку	
национални образовни програми и академски програми	
механизми за покретање иницијатива	
самостална индустрија сајбер безбедности	
Сарадња	
унутардржавна сарадња	
мултилатерални споразуми	
учешће у међународним форумима	
јавно-приватно партнерство	
партнерство између различитих агенција	

У Водичу кроз информациону безбедност у Србији из 2017. године каже се да Република Србија у процесу приступања Европској унији у области информационе безбедности приликом развоја нормативног оквира за регулисање ове области, треба да прати постојеће законодавство ЕУ, а посебно кровне прописе као што су Директива о мерама за обезбеђивање највећег нивоа

безбедности мрежних и информационих система широм ЕУ (2016), Конвенција о сајбер криминалу Савета Европе (2001), Стратегија сајбер безбедности ЕУ, Стратегија јединственог дигиталног тржишта ЕУ, Европска агенда безбедности и друге (Rizmal i dr, 2017:21). У том смислу, Закон о информационој безбедности[9] из 2016. године, први је закон те врсте „који регулише мере заштите од безбедносних ризика у информационо-коумникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система, те одређује надлежне органе за спровођење мера заштите“ (Rizmal i dr, 2017:33).

Кад су технички захтеви у питању, успостављање *Националног центра за превенцију безбедносних ризика у ИКТ системима* (Национални CERT)[10], које је било предвиђено Законом о информационој безбедности који је усвојен јануара 2016, реализовано је јануара 2017. године, те тај податак није уврштен у GCI скор за други (технички) стуб пошто је истраживање спровођено крајем 2016. године. Овај закон такође успоставља *Тело за координацију послова информационе безбедности*, које би сачињавали представник Министарства трговине, туризма и телекомуникација, представник Министарства одбране, представник Министарства унутрашњих послова, представник Министарства спољних послова, представник Министарства правде, представници служби безбедности (Безбедносно-информативне агенције, Војнобезбедносне агенције и Војнообавештајне агенције), представници Канцеларије Савета за националну безбедност и заштиту тајних података, представници Генералног секретаријата Владе Републике Србије, CERT-а републичких органа и Националног CERT-а (члан 5 Закона). Од информација које су битне за досадашњи рад Националног CERT-а Републике Србије може се издвојити да је новембра 2017. године укључен у међународну платформу за подршку активностима центара за реаговање на угрожавање безбедности информационих система, *Trusted Introducer*.

У погледу стандардизације, Закон о информационој безбедности предвиђа да се посебном уредбом пропише садржај Акта о безбедности ИКТ система од посебног значаја[11], али да је поред тога потребно „јасно прописати критеријуме за дефиницију инцидената у смислу врсте и значаја, како би се обезбедила вежа безбедност и ефикаснија размена информација, али и реаговање на саме инциденте“ (Rizmal i dr, 2017:42). На крају, кад је у питању сарадња, односно комуникација, најзначајније линије комуникације за повећање нивоа сајбер безбедности су оне између самих CERT-ова (посебно државних и приватних), као и између CERT-ова и успостављених регулаторних тела. Комуникација, поред тога што технички унапређује ниво сајбер безбедности, обезбеђује и адекватан и правовремен одговор на сајбер инциденте.

ЗАКЉУЧАК

Сајбер безбедност на почетку 21. века представља незаобилазни део свакодневнице која нам на великом броју примера показује да је због међусобне

[9] Службени гласник Републике Србије, бр. 6/16, 94/17.

[10] Национални CERT у надлежности је Регулаторне агенције за електронске комуникације и поштанске услуге (РАТЕЛ).

[11] Уредба о ближем садржају Акта о безбедности информационо-комуникационих система од посебног значаја, начину провере и садржају извештаја о провери безбедности информационо-комуникационих система од посебног значаја, Службени гласник Републике Србије, бр. 94/16.

зависности практично свих информационих и комуникационих мрежа, данас све могуће угрозити, у распону од права на приватност до великих система критичне инфраструктуре. Иако је број актера који имају одговорност за сајбер безбедност огроман, државе и даље носе највећи терет у погледу обавезе да доносе политике за унапређење безбедности које ће моћи да прате убрзани развој технологија, а да притом успевају да заштите своје информационе и комуникационе капацитете од значаја за националну безбедност.

Треба имати на уму да је Индекс глобалне сајбер безбедности релативно нов пројекат који, иако иза њега стоји међународна организација која окупља скоро све државе чланице Уједињених нација, и даље у доброј мери користи секундарне показатеље за изражавање вредности Индекса, као и за рангирање држава. Истраживачи из ITU су за потребе проверавања поузданости резултата из истраживања за развој Индекса глобалне сајбер безбедности 2017 са показатељима у релевантним областима, извршили поређење GCI са Индексом развоја ИКТ (*ICT for Development Index, IDI*), који такође развија ITU. Упоређивање резултата није открило директну везу између GCI и степена развоја ИКТ, јер искуство показује да земље које имају високе резултате када је у питању развој ИКТ не улажу пропорционално у сајбер безбедност, и обрнуто. Тако многе земље имају значајно бољи скор GCI него што то ниво развоја њихових информационих и комуникационих технологија показује (ITU, 2017:19). У другом истраживању, аутори са Универзитета Бредфорд анализирали су GCI 2014 скорове држава у односу на културалне димензије својствене свакој држави. Утврдили су да постоји корелација између развоја сајбер безбедности и културолошких димензија индивидуализма и оријентације ка дугорочним циљевима (Onumo et al., 2017).

Различита искуства држава указују на чињеницу да постоји и више различитих начина да се унапреди ниво сајбер безбедности на националном нивоу, а да то истовремено буде усклађено са непосредним и ширим окружењем (видети: Yunis & Koong, 2015), међутим, за све државе које планирају да унапреде своје системе сајбер безбедности, захтеве из постојећих пет стубова потребно је развијати подједнаком брзином и истовремено, уколико је то могуће. Због тога је кључни циљ Индекса глобалне сајбер безбедности изградња капацитета на националном, регионалном и међународном нивоу кроз процену степена ангажовања држава око сајбер безбедности, као и израда листе примера добре праксе која се може користити у државама којима је потребна помоћ у овој области.

ЛИТЕРАТУРА

1. Dimitrijević, R.I. & Stekić, N. (2018). „Intelligence Analysis Models for Asymmetric Threats“. In: Stojanović, S. (Ed.) (2018). Asymmetry and Strategy. Belgrade: Strategic Research Institute & National Defence School, pp. 653-668.
2. IISS (2015). The Military Balance 2015: The Annual Assessment of Global Military Capabilities and Defence Economics. London: The International Institute for Strategic Studies.
3. ITU (2017). Global Cybersecurity Index (GCI) 2017. Geneva: International Telecommunication Union.
4. ITU (April 2015). Global Cybersecurity Index & Cyberwellness Profiles (Report). Geneva: International Telecommunication Union.

5. Kuerbis, B. & Badiei, F. (2017). Mapping the Cybersecurity Institutional Landscape. Digital Policy, Regulation and Governance, 19(6), 466-492.
6. Mitrović, M. (2017). „Hybrid Security Threats and Contemporary Approach to National Security“. In: International Conference “Archibald Reiss Days” Proceedings (Vol. 1). Belgrade: Academy of Criminal and Police Studies, pp. 323-331.
7. Onumo, A., Cullen, A. & Awan, I.U. (2017). “Empirical Study of Cultural Dimensions and Cybersecurity Development”. The 5th International Conference on Future Internet of Things and Cloud, August 21-23, 2017, Prague.
8. Peng, S. (2015). Cybersecurity Threats and the WTO National Security Exceptions. Journal of International Economic Law, doi: 10.1093/jiel/jgv025.
9. Rizmal, I., Radunović, V. & Krivokapić, Đ. (2017). Vodič kroz informacionu bezbednost u Republici Srbiji. Beograd: Centar za evroatlantske studije i Misija OEBS-a u Srbiji.
10. Shafqat, N. & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. International Journal of Computer Science and Information Security, 14(1), 129-136.
11. Standish, R. (January 18, 2018). Inside a European Center to Combat Russia’s Hybrid Warfare. Foreign Policy, доступно на: http://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare/ (приступљено 1. марта 2018. године).
12. Yunis, M.M. & Koong, K.S. (2015). “A Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework”. Twenty-first Americas Conference on Information Systems, August 13-15, 2015, Puerto Rico.

CYBER THREATS INDICATORS:
THE ANALYSIS OF GLOBAL CYBERSECURITY INDEX

Ivan R. Dimitrijević
Faculty of Security Studies, University in Belgrade

Ana Paraušić
Faculty of Security Studies, University in Belgrade

Abstract: The importance of networks, devices, and services for information and communication technologies (ICT) today is obvious and crucial for regular functioning of almost all of the world countries. Around half of the world population has used the Internet in 2016, and it is estimated that by 2020 around 12 billion devices will be connected online, directly or via other devices. It is clear that there is a causal relation between the growth of information and communication technologies and their illegal or malicious use. This is the reason why almost every country in the world developed strategies for raising the level of their cyber security. However, there are still big differences between countries regarding the awareness, understanding, knowledge, and capacities for implementation of appropriate strategies and programs so that appropriate use of ICT is secured.

That is why the International Telecommunication Union (ITU), together with partners from public-private and private sectors, as well as with academia, has built the Global Cybersecurity Index (CGI). The key goal of the Index is capacity-building on national, regional, and international levels through assessment of the level of countries' engagement regarding the cyber security, as well as the development of the best practices examples list that could be used in countries which need support in this area.

The GCI started in 2014, when the first research was conducted among the ITU member-states, and it is based on so-called five pillars making the Global Cybersecurity Agenda (CGA). In our analysis, we will use the data and reports from the International Telecommunication Union, and besides the Global Cybersecurity Index 2014 and Global Cybersecurity Index 2017, we will use individual cybersecurity profiles of the European ITU member-states, with focus on the Republic of Serbia. We will analyze which threats are recognized in the cybersecurity area, and how are the ITU member-states prepared for dealing with these threats.

Key words: cyber threats, cyber security, Global Cybersecurity Index.