УДК 316.422:004.056
DOI: 10.5937/pr89-69211
Прегледни рад

Политичка ревија
3/2026.
Vol. 89
стр. 41-68

Слађана Ћурчић*

Институт за европске студије, Београд

САЈБЕР БЕЗБЕДНОСНА КУЛТУРА КАО ФЕНОМЕН РЕФЛЕКСИВНЕ МОДЕРНИЗАЦИЈЕ У ДРУШТВУ РИЗИКА: ПРИМЕНА КОНЦЕПЦИЈЕ УЛРИХА БЕКА

Сажетак

Рад се бави критичким посматрањем сајбер безбедносне културе кроз теоријску визуру социолога Улриха Бека (*Ulrich Beck*). Конкретно, рад ангажује теорију рефлексивне модернизације и концепт друштва ризика, са циљем објашњења сајбер ризика и сајбер безбедносне културе кроз ширу социолошку перспективу. Тумачењем сајбер ризика у светлу Бекове теоријске перспективе, овом анализом се аргументује поглед на сајбер безбедносну културу као део процеса рефлексивне модернизације, који се одвија у сајбер ризичном друштву, у великој мери детерминисаним технолошким напретком и убрзаним развојем вештачке интелигенције. Закључује се да посматрање сајбер безбедносне културе кроз Беков теоријски оквир не имплицира потпуну експланаторну моћ истог, али допуњује постојеће истраживачке напоре у интердисциплинарном

* Имејл: sladjana.curcic@ies.rs; ORCID: 0000-0001-8276-0983.

сагледавању концепта сајбер безбедносне културе. Наиме, позиционирањем проблематике сајбер безбедности у социолошки оквир, који је широко коришћен и у студијама безбедности, пружен је допринос досадашњим истраживањима сајбер безбедносне културе, која претежно почивају на технички оријентисаним, психолошким и организационим приступима.

Кључне речи: сајбер безбедносна култура, сајбер ризици, друштво ризика, рефлексивна модернизација, Улрих Бек

УВОД

Технолошки напредак и развој вештачке интелигенције, донели су значајне промене на глобалном нивоу и трансформисали свакодневни живот појединца, али и донели низ изазова у дигиталној, односно сајбер сфери. Сајбер безбедност постаје преокупација за државу, организације и појединце, на тај начин да сваки од наведених актера може утицати на сајбер безбедност оног другог, али истовремено може бити и извор претње. Наиме, државни актери могу спроводити сајбер нападе или сајбер шпијунажу према другим актерима из политичких, војних, идеолошких и других разлога. Приватне организације могу искоришћавати рањивости система различитих институција или других организација зарад финансијске или друге користи, док појединци намерно или ненамерно могу такође бити извор претњи по друге актере (Hansen and Nissenbaum 2009; Bishop 2025). Тако ширење домета и могућности у ери дигитализације и вештачке интелигенције, захтева и ширење одговорности сваког од нас за правилну, етичку и безбедну употребу алата који су нам располагању. Другим речима, захтева се виши ниво освешћености о стварним и потенцијалним ризицима и виши степен развијености сајбер безбедносне културе.

Стога, сајбер безбедносна култура постаје један од одговора на ризике које је човек сам произвео унапређујући дигиталну технологију.

Важност људског фактора у сајбер безбедности, па тако и сајбер безбедносној култури, довео је до ангажовања различитих теоријских приступа у разумевању овог феномена, попут социо-техничких и различитих психолошких приступа. Један од могућих, иако нетипичних погледа на проблематику сајбер безбедности, јесте теорија ризичног друштва немачког социолога Улриха Бека (*Ulrich Beck*). Нетипичност се огледа у томе што се сајбер безбедност, иако традиционално фокусирана на заштиту техничке инфраструктуре и осетљивих података, данас суочава са ширењем претњи ван уско схваћене материјалне сфере, укључујући аспекте људске и социјеталне безбедности (Domalewska, Gasztold, and Wrońska 2025). То изискује ширу перспективу која омогућава сагледавање и контекста и образаца дате појаве.

У студијама безбедности Беков теоријски приступ је примењиван у истраживању различитих појава и то, како сумирају поједини аутори, обично на један од три начина: као поткрепљење ставу да живимо у временима појачаних ризика, као основа за аргументацију који противречи Бековим сопственим тврдњама (реч је о приступима који ризик схватају као технологију владања) и најзад, Беков приступ се неретко примењује као потенцијално бољи експланаторни оквир за одређена питања безбедности, као што је нпр. рат, у односу на друге теорије (Selchow 2016). Примена Бекове концепције космополитизованог света показала се корисном и у анализи питања националне безбедности, пруживши перспективу о космополитизованој природи националне безбедности САД, коју обликује међусобно дејство два наизглед искључива аспекта космополитизованог света – „космополитизована реалност" и „традиција националне перспективе" (382).

Поједини аутори такође виде сајбер безбедност као појаву коју је погодније шире сагледавати из перспективе

друштва ризика и рефлексивне модернизације, у односу на традиционално коришћене теорије безбедности у овој области (Kook 2018). С обзиром на ширину Бековог теоријског опуса, аутори указују на постојећа истраживања која се баве важним питањем – да ли се његова теоријска перспектива мора у потпуности применити или је могуће анализирати конкретне феномене у „Бековом духу" или пак, изоловати и користити поједине аспекте његовог богатог рада (Selchow 2016). Овај рад свакако не представља тестирање или потпуну примену Бекове теорије, већ је ближи анализи у духу његове теоријске визуре и сагледавању и тумачењу сајбер безбедносне културе кроз оквир конкретних концепата, као што су друштво ризика и рефлексивна модернизација.

Рад је структурисан на следећи начин: у првом поглављу су приказане основе Бекове теорије рефлексивне модернизације и друштва ризика, уз преглед најчешћих примена Бекове теоријске перспективе у области безбедности; следи поглавље о теоријским приступима области сајбер безбедности, које укључује и схватања сајбер безбедносне културе, прожета тумачењима из угла ризичног друштва. Централно поглавље посвећено је сагледавању сајбер безбедносне културе у савременом ризичном друштву и тумачењу исте као феномена рефлексивне модернизације. У последњем поглављу сумирају се кључни увиди рада и ограничења анализе сајбер безбедносне културе кроз Бекову теоријску перспективу.

ТЕОРИЈА РЕФЛЕКСИВНЕ МОДЕРНИЗАЦИЈЕ И ДРУШТВО РИЗИКА

Научни рад Улриха Бека је у литератури неретко посматран као комплексан социолошки оквир, који укључује међусобно повезане концепте и теорије, почевши од теорије рефлексивне модернизације (Beck 1992; Beck, Bons, and Lau 2003), друштва ризика (Beck 1992), глобалног друштва ризика (Beck 1999), космополитизма (Beck 2006),

индивидуализације, глобализације (Beck and Beck–Gernsheim 2001) и другог. Поједини аутори његов широк опус тумаче као социолошку теорију о модернизацији и ризику (Kook 2018). Бек објашњава да се теорија рефлексивне модернизације може разложити на три теореме – теорему ризичног друштва, форсиране индивидуализације и теорему вишедимензионалне глобализације, односно космополитизације (Bek 2011). Све три теореме се међусобно оснажују и замишљене су као радикализоване форме динамике модернизације, која, примењена на саму себе на прелазу у 21. век, замењује формулу једноставне модерности (31). Свакако, не би било погрешно закључити да су сви наведени концепти и идеје, као и оне којима се Бек бавио у каснијем раду, међусобно прожети и релевантни за његов целокупан теоријски опус.

Суштински реч је о широком социолошком приступу са значајним референцама и доприносом за област безбедности. Наиме, како уочавају и други аутори, врло опсежан Беков рад о ризичном друштву своју утицајност показује кроз прелажење дисциплинарних граница и прожимање литературе о међународној политици и студијама безбедности, с обзиром на то да адресира теме, као што су еколошке претње, тероризам, нуклеарне катастрофе и друго (Kook 2018). У оквиру Бекове теоријске перспективе, за потребе овог рада издвајају се два уско повезана концепта релевантна за проблематизацију сајбер безбедносне културе: друштво ризика и рефлексивна модернизација.

Бек (Bek 2011) у свом раду истиче да је „теорија светског ризичног друштва друштвено-теоријски појам који има смисла само у контексту теорије рефлексивне модернизације као теорије самотрансформације модерног друштва" (79–80). Дакле, сам концепт ризика је директно повезан са концептом рефлексивне модернизације, будући да су ризици, за разлику од ранијих опасности које су углавном споља индуковане, настали као део процеса модернизације и индустријализације и у том смислу су политички рефлексивни, јер се друштво

суочава са самим собом, односно ненамерним споредним ефектима сопственог напретка и знања, а који временом постају свеприсутни (Beck 1992; Beck, Bons, and Lau 2003). Технолошки напредак поново служи као добар пример, нарочито у контексту развоја вештачке интелигенције, будући да је савременом човеку донео бројне могућности, али и све више ризика, свести о постојећим и потенцијалним ризицима у будућности. Међутим, „рефлексивно" у рефлексивној модернизацији не имплицира повећање свести људи и њиховог овладавања ризицима, већ појачану свест да је овладавање заправо немогуће (Latour 2003, цитирано у: Beck, Bons, and Lau 2003, 3). Сходно томе, логика производње и дистрибуције ризика је оно што карактерише „рефлексивну" или „другу" модернизацију (модернизација индустријског друштва), за разлику од логике производње и дистрибуције богатства, која одликује „прву" или „класичну" модернизацију (модернизација традиције) (Beck 1992). Тако фаза рефлексивне модернизације представља нову фазу у којој напредак може да се претвори у самоуништење и у којој једна врста модернизације подрива и мења другу (Beck, Giddens, and Lash 1994).

Иако су се људи и раније суочавали са различитим ризицима, оно што је *differentia specifica* ризика у рефлексивној модернизацији, јесте парадокс развоја и напретка, који неминовно са собом носи ризике (Drabik 2022). Дакле, реч је о ризицима људског порекла, у односу на раније, најчешће природно изазване, што води и ка промени опште парадигме о ризику од реалистичке ка конструктивистичкој, од стварних ка перципираним ризицима (Sundberg 2024). Бек (Beck 1992) дефинише ризик као „системски начин суочавања са опасностима и несигурностима изазваним и уведеним самом модернизацијом" (21). У том смислу се ризично друштво односи на развој нових ризика, који почиње у другој половини 20. века, као што су питања еколошких криза и смањивања граница државе благостања (Bek 2011).

Међутим, Бек (Beck 1992) напомиње да оно што разликује ризично од индустријског друштва, нису само бављење ризицима, повећани квалитет и обим ризика, већ чињеница да, како се ризици све више научно интерпретирају, губи се њихова латентна природа, а структурни друштвени услови се радикално трансформишу услед рефлексивне модернизације.

Суштина, али и контрадикција ризичног друштва се огледа у томе, да се оно суочава са великим опасностима, које су последица успеха, а не пораза модерног друштва, а на које се не може одговорити у складу са важећим правним, научним и политичким принципима (Bek 2011). Наиме, модернизација, која се најбоље огледа у напретку технологије, осим што представља успех и достигнуће човечанства, истовремено генерише ризике на које више није могуће одговорити на, до сада познат, „традиционалан" начин. Бек (Bek 2011) иде још даље и проширује своју тезу на глобални ниво, односно, говорећи у оквирима светског ризичног друштва, указује на глобализацију ризика и немогућност основних институција модерне државе, науке и економије да им се супротставе и осигурају безбедност грађанима (72–73). Штавише, ови стубови модерне постају, не део решења, већ део проблема који би требало да реше, у чему се и огледа значење појма рефлексивна модернизација (83).

Теорије ризичног друштва и рефлексивне модернизације, примењивали су Бек и други аутори у проучавању разноврсних потенцијалних безбедносних ризика, али и реалних безбедносних претњи са којима се човечанство данас суочава. Међу њима су, како тзв. традиционална питања безбедности, попут нуклеарних катастрофа, тероризма (Bek 2011), рата (Heng 2006), тако и „ нетрадиционална" или невојна, као што су заразне болести (Elbe 2008), еколошке претње, технолошки ризици (Beck 1995, 2011). Сајбер безбедност привлачи пажњу, као једна од области која се такође може посматрати кроз призму теорије ризичног друштва и рефлексивне модернизације. Истраживања у овој области се крећу од

општих разматрања сајбер безбедности на темељима друштва ризика (Deibert and Rohozinski 2010; Kook 2018; Drabik 2022) и сајбер безбедносне културе (Bakić and Alispahić 2021), до изучавања изазова дигитализације савременог друштва (Rizkidarajat et al. 2023; Rughiniș et al. 2024; Sundberg 2024) и повезаности вештачке интелигенције и сајбер ризика (Vulpe et al. 2024) кроз призму теорије ризичног друштва. Приметно је да су оскудна истраживања која директније изучавају сајбер безбедносну културу кроз оквир рефлексивне модернизације, те стога постојећи корпус литературе, који на шири начин повезује сајбер безбедност и друштво ризика, пружа основ за даља истраживања у овом правцу.

САЈБЕР БЕЗБЕДНОСТ И САЈБЕР РИЗИЦИ У САВРЕМЕНОМ ДРУШТВУ РИЗИКА

Убрзан технолошки развој представља централну тачку дискусија о сајбер ризицима и сајбер безбедности. Другачије речено, сајбер безбедност оличава тежњу да се савремено друштво заштити од сајбер ризика које је само произвело унапређивањем и усавршавањем технологије. Парадокс који прожима ову тезу, даје довољан подстрек истраживачима студија безбедности, да идеју о управљању тим ризицима путем сајбер безбедносне културе, посматрају у светлу рефлексивне модернизације.

Зачеци сајбер безбедности као поља истраживања у студијама безбедности, везују се за касне седамдесете године 20. века (Dunn–Cavelty 2013), али свакако највећи замах ова област доживљава у ери убрзаног напретка савремених технологија. Иако је сајбер безбедност нераскидиво везана за виртуелни простор, свакако има шири обухват. Тако разнолика одређења појма сајбер безбедности, обједињује схватање да исти укључује и технички, људски, организациони и виртуелни аспект. Сходно томе, све је већи број аутора који имају критичко становиште према уско „технички-оријентисаним" одређењима сајбер безбедности, која фокус

стављају на политике, процедуре, мере, активности, средства и слично, занемарујући комплексност феномена (Craigen, Diakun–Thibault, and Purse 2014). Отуда је очигледно настојање ка пружању свеобухватних приступа, који одражавају вишедимензионалну природу сајбер безбедности и битну чињеницу да у сајбер простору људи могу истовремено бити и референтни објекат (предмет заштите) и извор претње по сајбер безбедност, свесно или несвесно (Hansen and Nissenbaum 2009; Domalewska, Gasztold, and Wrońska 2025). Према једном од таквих свеобухватних становишта, сајбер безбедност представља „заштиту самог сајбер простора, електронских информација, информационо-комуникационих технологија које подржавају сајбер простор и личне, друштвене и националне капацитете корисника сајбер простора, укључујући њихове интересе, било материјалне или нематеријалне, који су рањиви на нападе који потичу из сајбер простора". Сходно томе, циљ сајбер безбедности јесте обезбеђивање свих оних који функционишу у сајбер простору, било да су то појединци, организације, критична национална инфраструктура, друштва или нације (Von Solms and Van Niekerk 2013, 101).

Дакле, еволуцију у погледу дијапазона, врсте и софистицираности сајбер претњи, пратио је и развој у схватању сајбер безбедности. Тако се у литератури истиче да су традиционални ризици попут вируса и малвера усмерених на угрожавање рачунарских система или крађу осетљивих информација, еволуирали у широк спектар претњи глобалног карактера усмерених на људе, попут социјалног инжењеринга и дезинформисања (Lupton 2016; Domalewska, Gasztold, and Wrońska 2025). Читав спектар свих могућих сајбер ризика и претњи, укључујући и њихову класификацију, врло је тешко ограничити, будући да се константно умножавају са ширењем потенцијала савремених технологија. Свакако, неке од најозбиљнијих претњи, укључују сајбер нападе, сајбер криминал и сајбер тероризам, који имају последице по државе,

појединце, организације и критичну инфраструктуру (Luknar and Jovanović 2024). Другим речима, глобални карактер претњи чини рањивим субјекте свих нивоа – од индивидуалног, преко националног до међународног, а узевши у обзир и њихову умреженост, последице се преливају са једног на други ниво. У том светлу, поједини аутори указују на потенцијал сајбер безбедности, као „глобализујуће" политичке рационалности да критички трансформише и поткопа нормативне поретке и институционалне границе карактеристичне за либералне демократије, утемељене у раздвајању између унутрашње и спољне безбедности, између јавне и приватне сфере и између државе и друштва (Haddad and Binder 2019). Подривање или потпуно брисање наведених граница произилази из чињенице да је заправо сајбер простор немогуће јасно ограничити, што се посебно рефлектује на тешкоће у дефинисању сајбер безбедности на националном нивоу, јер је иста нужно детерминисана безбедношћу других актера, односно сајбер безбедношћу на глобалном нивоу (Kook 2018). Са друге стране, сајбер безбедност у, условно речено, националним оквирима, нераскидиво је повезана са индивидуалним нивоом. Наиме, поједине анализе указују и да се у државним стратегијама сајбер безбедности истиче индивидуална одговорност и допринос сваког грађанина унапређењу сајбер безбедности, кроз развој сајбер безбедносне културе, едукацију и освешћеност о ризицима у сајбер простору (Kook 2018; Haddad and Binder 2019).

Сложеност и слојевитост веза и интеракција на релацији људи–технологија, упућује на потребу широког сагледавања области сајбер безбедности, што подразумева интердисциплинарну комуникацију и укључивање и техничко-технолошке, правне, етичке, социјалне и психолошке димензије, као и узимање у обзир и културног контекста када се истражује одређено друштво (Domalewska, Gasztold, and Wrońska 2025; Luknar 2025). Бековим речима (Bek 2011, 28) сведочимо „сукобу ризичних култура", с обзиром да

се глобални ризици различито перципирају у различитим деловима света. Следствено вишедимензионалном карактеру дигиталних ризика, исти су изучавани из различитих теоријских перспектива, као што су дигитална социологија, студије интернета, студије надзора и нових медија и комуникација (Lupton 2016). У светлу напретка дигиталних технологија, Бек (Beck 2013) говори и о глобалним ризицима по дигиталне слободе, који као и други ризици, попут оних у вези са климатским променама, нуклеарном енергијом, финансијама, представљају пратеће ефекте успешне модернизације, која ретроспективно доводи у питање институције које су је управо подстицале. Узевши у обзир и вештачку интелигенцију која у значајној мери детерминише одлике сајбер ризика, као што су глобална и неједнака дистрибуција, комплексност, тешкоће у идентификовању обима и утицаја (Vulpe et al. 2024), може се рећи да наведене одлике кореспондирају обележјима глобалних ризика светског ризичног друштва које истиче Бек (Bek 2011), као што су делокализација, непрорачунљивост последица, ненадокнадивост штете (79).

Концепт сајбер безбедносне културе

Тешкоће у дефинисању сајбер безбедности, повлаче и изазове у одређењу концепта сајбер безбедносне културе. Настојање истраживача ка што комплетнијем сагледавању концепта, неретко резултира ослањањем на традиционалне перспективе организационе културе, попут Шејновог (*Edgar Schein*) модела организационе културе (Reegård, Blackett, and Katta 2019; Adamu 2023), модела информационе безбедносне културе (Adamu 2023), те и социо-психолошких оквира, попут интеграције институционалне теорије и теорије мотивације за заштитом (Andronache 2021), као и Куперовог (*Dominic Cooper*) модела реципрочног детерминизма заснованог на Бандуриној (*Albert Bandura*) социјално-когнитивној теорији (Ćurčić 2024). Такође, све је чешће и комбиновање технички

оријентисаних приступа са организационим и психолошким приступима, попут интеграције дисциплине информационих технологија са индустријском психологијом (Da Veiga 2016), што у потпуности одржава сложену природу феномена сајбер безбедносне културе.

Према једном од сложенијих схватања сајбер безбедносне културе, оквир за процену сајбер безбедносне културе подразумева организациони и индивидуални ниво, који су организовани у димензије, а димензије рашчлањене на домене (Georgiadou et al. 2022). Организациони ниво чини шест димензија: средства, континуитет, приступ и поверење, операције, одбрана и управљање безбедношћу, док индивидуални ниво чине следеће димензије: став, свест, понашање и компетентност (455). Већина дефиниција сајбер безбедносне културе, заправо представља организациону сајбер безбедносну културу, али све више аутора увиђа да је неопходно превазилажење организационог контекста имајући у виду карактер сајбер ризика (Reid and Van Niekerk 2014; Reegård, Blackett, and Katta 2019). Наиме, аутори који су развили модел информационе безбедносне културе на бази Шејновог модела организационе културе, указују да је сајбер безбедносна култура релевантна за шири друштвени контекст и сходно томе нуде перспективу размишљања о сајбер безбедносној култури и њеног разликовања од информационе (Reid and Van Niekerk 2014, 4). Кључна разлика се управо тиче контекста, где је друштвени контекст у којем се негује сајбер безбедносна култура мање контролисан, а активности појединаца мање предвидљиве за разлику од организационог. Друга разлика се односи на компоненте, које би се код сајбер безбедносне културе разликовале од информационе и другачије манифестовале у стварном окружењу, управо због сложенијег контекста (5–6).

Упркос споревима око дефиниције, релевантним за даљи теоријски развој концепта, суштина сајбер безбедносне културе, барем у практичном смислу је очигледна. Наиме,

сајбер безбедносна култура неспорно представља један од видова управљања претходно наведеним сајбер ризицима. Као и безбедносна култура уопште, сајбер безбедносна култура почива на превенцији, свести о стварним и потенцијалним ризицима и претњама, адекватној информисаности и знању о појединим изазовима сајбер безбедности, свести о личној одговорности за заштиту осетљивих података, заштиту система, софтвера и другог. Ниво развијености сајбер безбедносне културе демонстрирамо свакодневно, иако тога најчешће нисмо свесни – кроз електронску комуникацију, најчешће мејл, коришћење различитих софтвера, друштвених мрежа, апликација, попут мобилног банкарства, до осетљивијих питања, као што је активност родитеља на друштвеним мрежама, која укључује децу и самим тим повлачи питање њихове приватности и безбедности у дигиталној сфери. Све наведено изискује одређени ниво свести и културе о постојећим и могућим ризицима, а последње нарочито, јер захтева бригу и одговорност за малолетно лице и његову добробит, те и одређени ниво саморегулације, услед ограничених домета правне регулативе, која евидентно заостаје за убрзаним развојем савремених технологија (Novaković 2025). Дакле, примарно, сајбер безбедносна култура оличава индивидуалну „стратегију" заштите од разноврсних сајбер ризика. Са развојем и усавршавањем система и алата вештачке интелигенције, усложњавају се сајбер ризици, те тако и сајбер безбедносна култура добија нову димензију.

Наглашавање људске улоге, као критичног елемента или чак најслабије карике у сајбер сфери, постаје опште место у теоријским расправама о сајбер безбедности (Von Solms and Van Niekerk 2013; Domalewska, Gasztold, and Wroń**s**ka 2025). Наведено сугерише да је човек интегрална компонента „сајбер екосистема", да има активну, а не пасивну улогу, те да је људско понашање извор потенцијалних рањивости, али и фактор заштите у датом екосистему (Domalewska, Gasztold,

and Wrońska 2025). Активан допринос појединца унапређењу сајбер безбедности, управо се огледа у развијеној сајбер безбедносној култури. Ако се наведено посматра у претходно поменутом, ширем друштвеном контексту, то имплицира едуковане, дигитално писмене и оспособљене грађане, који се понашају одговорно и компетентно у сајбер простору (Haddad and Binder 2019). У том светлу, аспект културе ризика се односи на колективни напор да се негује безбедносна култура коју карактерише заједничка одговорност и проактиван став према сајбер претњама (Domalewska, Gasztold, and Wrońska, 2025). Узевши у обзир потребу за интердисциплинираним приступом у суочавању са сајбер ризицима и очигледан значај социолошке и психолошке перспективе, посматрање сајбер безбедносне културе кроз призму ризичног друштва, представља само један од углова који осветљава дати феномен.

САЈБЕР БЕЗБЕДНОСНА КУЛТУРА КАО ФЕНОМЕН РЕФЛЕКСИВНЕ МОДЕРНИЗАЦИЈЕ

Сајбер безбедносна култура, као што је већ истакнуто, превасходно одражава превентивни приступ у суочавању са сајбер ризицима. Превенција, а не реакција, представља и генералан заокрет у размишљању у студијама безбедности, посебно у постхладноратовском периоду суочавања са разноврсним, многобројним, квалитативно другачијим ризицима (Williams 2008). У светлу неизвесности глобалних ризика, Бек (Bek 2011) такође указује на вредносну хијерархију форми политичког деловања, где приоритет има проактивна политика у односу на реактивну. Поједини аутори, истичући инхерентно другачију природу сајбер безбедности, указују да концепт ризичног друштва пружа увиде о тој природи и њеној специфичности, који се могу чинити неухватљивим из угла традиционалних приступа безбедности (Kook 2018). Наведено се аргументује кроз примену концепта ризичног друштва у анализи начина на који политички лидери разумеју и концептуализују сајбер ризике и начина на који то утиче

на одлучивање и креирање стратегија у области сајбер безбедности (5).

Питање могућности управљања тзв. нетрадиционалним безбедносним ризицима, посебно долази до изражаја у сфери сајбер безбедности, која постаје комплекснија са напретком технологије. Сама тежња ка управљању ризицима, кроз сајбер безбедносну културу, одраз је свести човечанства о пратећим негативним ефектима модернизације, односно одраз је способности људи да промишљају о нуспојавама успеха модернизације (Beck 1992). Наиме, дигитализација и савремене технологије представљају решење одређених проблема у индустријском друштву, док истовремено стварају нове ризике као што су изазови сајбер безбедности, неодговорна употреба вештачке интелигенције, дигитални јаз и друго (Sundberg 2024). Тиме се поткрепљује теза да човечанство ствара нове параметре ризика кроз напредак, а сајбер ризици дефинитивно представљају нове параметре ризика у касној модерности, чинећи рањивим и велике информационе системе и појединца који свакодневно користи уређаје савремене технологије (Drabik 2022). Са друге стране, критика научног и технолошког прогреса, све присутнија у ери вештачке интелигенције и њој својствених ризика, према Беку (Beck 1992) није у супротности са модерношћу, већ је израз рефлексивне модернизације изван оквира индустријског друштва. У контексту сајбер ризика, може се рећи да је више реч о критици начина употребе савремених технологија, не и о противљењу модернизацији и напретку као таквим.

Водећи се Бековом (Bek 2011) тезом да је модерно друштво постало ризично друштво, јер је све јаче ангажовано у дебатама о самогенеришућим ризицима у покушају да их савлада и спречи (77) и у којем технологија има кључну улогу (Beck 1995), садашњи моменат развоја технологије, који је значајно одмакао од периода о којем Бек пише, пружа додатно упориште за тумачење сајбер безбедности у „Бековом кључу". Узевши у обзир и аргументацију да је

сајбер безбедност рефлексивне природе – јер је друштво свесно ризика које продукује константним унапређењем технологије, да антиципира ризике, предузима мере да се заштити од истих, али да се ризици не могу елиминисати, већ се могу само донекле контролисати (Kook 2018) – произилази да у таквој поставци, сајбер безбедносна култура представља део менаџмента сајбер ризицима. Будући да то не подразумева само капацитете појединца као такве, већ и знање како користити технолошке алате у сврху препознавања и заштите од ризика, поједини аутори иду и корак даље тврдећи да се у дигиталном ризичном друштву, технологија користи за решавање проблема изазваних самом технологијом (Sundberg 2024). Примери се могу наћи у свакодневном животу, попут софтвера за заштиту од потенцијалних сајбер напада или апликација за препознавање садржаја генерисаних вештачком интелигенцијом. Управо у ризицима повезаним са употребом вештачке интелигенције, неки истраживачи виде рефлексиван приступ управљању ризицима, који се огледа у идентификовању и отклањању рањивости у системима и алатима вештачке интелигенције, попут циклуса развоја, примене и процене утицаја *ChatGPT* алата и њему сличних (Vulpe et al. 2024). Полазећи од претпоставке да ће сајбер ризици наставити да се умножавају, услед континуираног и неповратног процеса напретка технологије и дигитализације (Kook 2018), аутори оцењују да ће последично еволуирати и методе и начини одговора на сајбер ризике (Rughiniș et al. 2024).

Са динамиком технолошког напретка и сајбер безбедносна култура ће добијати нове обрисе, захтевати нова прилагођавања на индивидуалном и ширем, друштвеном нивоу. Тако сајбер безбедносна култура представља један од могућих одговора на проблем са којим се суочава ризично друштво: како се ризици, систематски произведени процесом модернизације могу спречити, минимизирати и ограничити, тако да не ометају процес модернизације, нити

прелазе границе онога што је подношљиво у еколошком, медицинском, психолошком и социјалном смислу (Beck 1992, 19). Будући да Бек говори о контекстуално одређеним границама подношљивости, не и о конкретним „категоријама" подношљивих ризика, тако и сајбер безбедносна култура представља један од начина управљања сајбер ризицима, чија „граница подношљивости" није унапред јасно дефинисана, већ је такође детерминисана контекстом, могућим последицама, дометима савремене технологије и другим факторима. Другим речима, безбедносна култура се може посматрати као феномен рефлексивне модернизације, односно као пракса, механизам и стратегија коју континуирано треба унапређивати и прилагођавати динамичном сајбер окружењу. Друштво сајбер ризика у овом контексту, представља друштво суочено са ризицима које доносе аутоматизација и нове технологије, као ненамерним последицама модернизације. Развојем сајбер безбедносне културе на индивидуалном и колективном нивоу, спречавају се потенцијално већи ризици, који могу имати озбиљне последице по национални и међународни ниво. На пример, услед растуће међузависности у сајбер сфери, мањи проблем дигиталне безбедности у објектима критичне инфраструктуре, попут нуклеарне електране, може да изазове озбиљне проблеме нуклеарне безбедности, који се даље могу прелити на шири енергетски сектор, проузрокујући потом застој у снабдевању електричном енергијом, у транспорту, комуникацијама, па и друштвене немире (Haddad and Binder 2019).

Наведени пример представља такву врсту опасности, за коју Бек тврди да, ако би се реализовала, касније деловање би било практично немогуће. Стога, он истиче да центар свести о ризику лежи у будућности, не у садашњости, јер пројекције потенцијалне будућности обликују превентивне акције у садашњости (Beck 1992, 34). Према Бековом схватању (Bek 2011), независно од тога да ли живимо у свету који је „објективно" безбеднији од свих претходних, антиципација

такве катастрофе у сајбер сфери, обавезује на превентивно деловање. То последично повлачи стално бављење друштва сајбер ризицима, њихово стално предвиђање, у тежњи да се буде корак испред ризика, да се буде у приправности у случају да се ти ризици реализују.

Суочавање са таквом неизвесношћу постаје део свакодневице на индивидуалном, а нарочито на организационом нивоу у друштву сајбер ризика. Наиме, организације подстичу сталну едукацију, тренинг и усавршавање вештина запослених у области сајбер безбедности, чиме се обликују њихови ставови и понашање и тиме унапређује сајбер безбедносна култура (Lie, Utomo, and Winarno 2021). Тако се запослени обучавају да препознају потенцијалне сајбер ризике и благовремено реагују, те тако у друштву ризика, према Беку (Bek 2011) опажање објективних ризика у великој мери постаје ствар субјективне перцепције, расуђивања и разумевања (28). Са друге стране, виши ниво освешћености о потенцијалним сајбер ризицима и јачање капацитета за реаговање на исте, може створити осећај самоуверености, што одражава амбивалентну и динамичну интеракцију између стварних и перципираних ризика (Rughiniș et al. 2024). Додатни парадокс уноси вештачка интелигенција као неизоставна компонента сајбер ризика, будући да одбрана од таквих ризика и претњи, захтева алате и системе такође базиране на вештачкој интелигенцији (Vlada Republike Srbije 2025). У целини, сајбер безбедносна култура одражава много већу одговорност појединца, с обзиром да држава, као традиционални провајдер безбедности, у друштву ризика не може да осигура безбедност грађана (Bek 2011), а нарочито сајбер безбедност у околностима убрзаног технолошког развоја, дифузних, бројних и софистицираних сајбер ризика.

ЗАКЉУЧАК

Анализа сајбер безбедносне културе, теоријски утемељена у концепту друштва ризика и рефлексивне модернизације, имала је за циљ да пружи један од могућих погледа на овај савремени изазов, нарочито у ери вештачке интелигенције. Сајбер безбедносна култура, централни концепт овог рада, посматрана је као феномен рефлексивне модернизације, односно као превентивна пракса, стратегија и одраз свести људи о самопроизведеним ризицима у сајбер ризичном друштву. Ненамерни, споредни ефекти модернизације који је требало да буду ужи по обиму, латентни, временом су постали глобални и добили централни значај у друштвеним и политичким дебатама, а последице техничке револуције којој сведочимо, управо су један од најзначајнијих споредних ефеката модернизације (Beck 1992; Beck, Bonss, and Lau 2003). Сајбер ризици су очигледан пратећи ефекат савременог дигиталног доба, те тиме и предмет научних истраживања, важно питање у организацијама, високој политици и свакодневном животу. Значај за сваки ниво анализе, одражава поменуто преливање сајбер претњи, односно илуструје како дискурс о сајбер безбедности фигурира између индивидуалне и колективне безбедности, између јавних власти и приватних институција и између економске и политичко-војне безбедности (Hansen and Nissenbaum 2009).

С обзиром на већ поменуту ширину и макро ниво Бековог теоријског приступа, овај рад свакако не претендује да исти представи као комплетан експланаторни оквир за питање сајбер ризика и сајбер безбедносне културе, већ као оквир који нуди одређене елементе и концепте који помажу у критичком сагледавању испитиваног феномена. Шира социолошка перспектива сајбер безбедносне културе, свакако допуњује постојеће приступе, претежно психолошки, организационо-технички оријентисане. Додатно, ограничење

ове анализе огледа се и у немогућности да обухвати и прикаже све премисе теорије рефлексивне модернизације које поткрепљују идеју о сајбер безбедносној култури, као феномену тог процеса, већ скицира само кључне тезе, те овај рад треба схватити и као потенцијално отварање простора за даље анализе у овом правцу.

Постоје и одређене критике Бековог рада, од којих једна лежи управо у ширини његове теоријске перспективе, која је истовремено истицана и као позитиван аспект. Наиме, поједини аутори Беков теоријски приступ виде као нејасан, што такође отвара могућност широке интерпретације, али и манипулације (Kook 2018). Други истраживачи, такође, уочавају провизорност у Бековом раду која се тиче недоследне терминологије и преплитања појмова, али која је инхерентна целокупном његовом приступу. Међутим, како се истиче, та провизорност не значи нужно недостатак, већ одражава амбивалентност света који он описује, те тако истраживања инспирисана Бековим радом, такође садрже елементе те провизорности (Selchow, 2016). Сам Бек у једном од радова (Beck 1992) указује да се његова анализа не одвија у складу са емпиријским друштвеним истраживањима, већ тежи да сагледа обрисе будућности која тек почиње да се обликује (друштво ризика), у односу на још увек доминантну прошлост (индустријско друштво), те је његова теорија пројективна, али без чврсте методолошке потпоре. Стога, ако се прихвати да се провизорност Бековог приступа рефлектује и на овај рад, то није само због теоријског полазишта, већ и природе сајбер безбедности, која представља динамично поље континуираних промена, те док садашњи моменат у којем се налазимо већ делује довољно комплексан, пројекција будућности је неухватљива. Због тога „дијагноза" садашњег тренутка у домену сајбер безбедности, подсећа на Бекову оцену да смо „истовремено и субјекти и објекти" (Beck 1992, 9), односно сведоци времена убрзане аутоматизације и дигитализације рада и живота, који смо произвели и чије

ефекте доживљавамо свакодневно. Као што истичу поједини аутори, свакодневним безбедносним активностима појединци утичу на сајбер безбедност на ширем нивоу (Hansen and Nissenbaum 2009), те стога сајбер безбедносна култура остаје релевантна тема научних истраживања и пракса коју свакодневно треба унапређивати, сходно променама у сајбер сфери.

РЕФЕРЕНЦЕ

Adamu, Meseret Assefa. 2023. "Conceptualizing and Learning to Foster Cybersecurity Culture: A Literature Review". In *The 15th Mediterranean Conference on Information Systems (MCIS) Proceedings*, Madrid, 2023. https://aisel.aisnet.org/mcis2023/16/.

Andronache, Alina. 2021. "Increasing Security Awareness through Lenses of Cybersecurity Culture". *Journal of Information Systems and Operations Management* 15 (1): 7–22.

Bakić, Sarina, and Bakir Alispahić. 2021. "Phenomenology of Cyber Security Culture in the Context of Risk Society." *SunText Review of Arts and Social Sciences* 2 (1): 1–4. DOI: 10.51737/2766-4600.2021.01.

Beck, Ulrich, and Elisabeth Beck-Gernsheim. 2001. *Individualization: Institutionalized individualism and its social and political consequences.* London: SAGE Publications.

Beck, Ulrich, Anthony Giddens, and Scott Lash. 1994. *Reflexive modernization: Politics, tradition and aesthetics in the modern social order*. Stanford: Stanford University Press.

Beck, Ulrich, Wolfgang Bonss, and Christoph Lau. 2003. "The Theory of Reflexive Modernization: Problematic, Hypotheses and Research Programme". *Theory, Culture & Society* 20 (2): 1–33. DOI: 10.1177/0263276403020002001.

Beck, Ulrich. 1992. *Risk Society: Towards a New Modernity*. London: Sage Publications.

Beck, Ulrich. 1995. *Ecological Politics in an Age of Risk.* (Translated by Amos Weisz). Cambridge: Polity Press.

Beck, Ulrich. 1999. *World Risk Society*. Cambridge: Polity Press.

Beck, Ulrich. 2006. *The Cosmopolitan Vision.* Cambridge: Polity Press.

Beck, Ulrich. 2013. "The digital freedom risk: to fragile an acknowledgement". *OpenDemocracy*. August 30, 2013. https://www.opendemocracy.net/can-europe-make-it/ulrichbeck/digital-freedom-risk-too-fragile-acknowledgment.

Bek, Ulrih. 2011. *Svetsko rizično društvo. U potrazi za izgubljenom sigurnošću*. (Prevod sa originalnog izdanja na nemačkom iz 2007). Novi Sad: Akademska knjiga.

Bishop, Gulsebnem. 2025. *Cybersecurity culture*. Abingdon, Boca Raton: CRC Press (Taylor & Francis Group).

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014. "Defining Cybersecurity". *Technology Innovation Management Review* 4 (10): 13–21. DOI: 10.22215/timreview/835.

Ćurčić, Slađana. 2024. "Cybersecurity Culture from the Perspective of Social Cognitive Theory: Examining the Relevance of the Reciprocal Determinism Model". In *Navigating the Digital Age: An In-Depth Exploration into the Intersection of Modern Technologies and Societal Transformation,* eds. Ljubiša Bojić, Simona Žikić, Jörg Matthes and Damian Trilling, 377–406. Belgrade: Institute for Philosophy and Social Theory, University of Belgrade, University of Vienna, Department of Communication. DOI: https://doi.org/10.5281/zenodo.14204694.

Da Veiga, Adéle. 2016. "A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument". In *2016 SAI Computing Conference (SAI)*:1006–1015. DOI:10.1109/SAI.2016.7556102.

Deibert, Ronald J., and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security". *International Political Sociology* 4 (1): 15–32. DOI: 10.1111/j.1749-5687.2009.00088.x.

Domalewska, Dorota, Aleksandra Gasztold, and Agnieszka Wrońska. 2025. *Humans in the Cyber Loop: Perspectives on Social Cybersecurity*. Leiden: Brill. DOI: 10.1163/9789004549906.

Drabik, Krzysztof. 2022. "Cyberspace in a Risk Society". *Cybersecurity and Law* 7 (1): 17–26. DOI: 10.35467/cal/151808.

Dunn–Cavelty, Myriam. 2013. "Cyber-security". In *Contemporary Security Studies*, ed. Alan Collins. 362–378. Oxford: Oxford University Press.

Elbe, Stefan. 2008. "Risking Lives: AIDS, Security and Three Concepts of Risk". *Security Dialogue* 39 (2–3): 177–198. DOI: 10.1177/096701060808877.

Georgiadou, Anna, Spiros Mouzakitis, Kanaris Bounas, and Dimitris Askounis. 2022. "A cyber-security culture framework for assessing organization readiness". *Journal of Computer Information Systems* 62 (3): 452–462. DOI: 10.1080/08874417.2020.1845583.

Haddad, Christian, and Clemens Binder. 2019. "Governing through Cybersecurity: National Policy Strategies, Globalized (In-) Security and Sociotechnical Visions of the Digital Society". *Österreichische Zeitschrift für Soziologie* 44 (suppl. 1): 115–134. DOI: 10.1007/s11614-019-00350-7.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53 (4): 1155–1175. DOI: 10.1111/j.1468-2478.2009.00572.x.

Heng, Yee-Kuang. 2006. "The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society". *International Relations* 20 (1): 69–91. DOI: 10.1177/0047117806060929.

Kook, Lauren. 2018. "Cyber Security and Risk Society: Estonian Discourse on Cyber Risk and Security Strategy". Master thesis. University of Tartu, Estonia: Faculty of Social Sciences.

Lie, Laksana Budiwiyono, Prio Utomo, and P. M. Winarno. 2021. "Investigating the Impact of Cybersecurity Culture on Employees' Cybersecurity Protection Behaviours: A Conceptual Paper". *Conference Series* 3 (2): 295–305. DOI: 10.34306/conferenceseries.v3i2.598.

Luknar, Ivana. 2025. *Socio-political effects of technology*. Belgrade: Institute for Political Studies.

Luknar, Ivana, and Filip Jovanović. 2024. "Various types of cyber threats". *Srpska politička misao* 83 (1): 161–177. DOI: 10.5937/spm83-46059.

Lupton, Deborah. 2016. "Digital Risk Society". In *The Routledge Handbook of Risk Studies*, eds. Adam Burgess, Alberto Alemanno and Jens Zinn. 301–309. London: Routledge.

Novaković, Uroš. 2025. „Pravna regulacija prikazivanja dece na internetu i društvenim mrežama od strane roditelja–teorijski i praktični aspekt". *Politička revija* 85 (3): 45–61. DOI: 10.5937/pr85-60418.

Reegård, Kine, Claire Blackett, and Vikash Katta. 2019. "The Concept of Cybersecurity Culture". In *The 29th European Safety and Reliability Conference (ESREL 2019)*: 4036–4043. DOI: 10.3850/978-981-11-2724-3_0761-cd.

Reid, Rayne, and Johan Van Niekerk. 2014. "From Information Security to Cyber Security Cultures". In *13th Conference on Information Security for South Africa (ISSA 2014)*: 1–7. Johannesburg: IEEE. DOI: 10.1109/ISSA.2014.6950492.

Rizkidarajat, Wiman, Isna Hanny Puspaningtyas, Nethania Romauli, and Aulia Putri Maharani. 2023. "Contextualization of Risk Society in the Reality of Digital Work in Purwokerto, Central Java, Indonesia". *Revista Nuestramerica* 12 (22): 1–22. DOI: 10.5281/zenodo.10627713.

Rughiniș, Răzvan, Emanuela Bran, Ana Rodica Stăiculescu, and Alexandru Radovici. 2024. "From Cybercrime to Digital Balance: How Human Development Shapes Digital Risk Cultures". *Information* 15 (1): 1–17. DOI: 10.3390/info15010050.

Selchow, Sabine. 2016. "The Paths Not (Yet) Taken: Ulrich Beck, the 'Cosmopolitized World' and Security Studies". *Security Dialogue* 47(5): 369–385. DOI: 10.1177/0967010616647859.

Sundberg, Leif. 2024. "Towards the Digital Risk Society: A Review". *Human Affairs* 34 (1): 151–164. DOI: 10.1515/humaff-2023-0057.

Vlada Republike Srbije. 2025. *Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025–2030. godine.* Beograd: Vlada Republike Srbije.

Von Solms, Rossouw, and Johan Van Niekerk. 2013. "From Information Security to Cyber Security". *Computers & Security* 38 (7): 97–102. DOI: 10.1016/j.cose.2013.04.004.

Vulpe, Simona-Nicoleta, Răzvan Rughiniș, Dinu Țurcanu, and Daniel Rosner. 2024. "AI and Cybersecurity: A Risk Society Perspective". *Frontiers in Computer Science* 6 (2024): 1–11. DOI: 10.3389/fcomp.2024.1462250.

Williams, Michael J. 2008. "(In)Security Studies, Reflexive Modernization and the Risk Society". *Cooperation and Conflict* 43 (1): 57–79. DOI: 10.1177/0010836707086737.

Slađana Ćurčić*
Institute of European Studies, Belgrade

CYBERSECURITY CULTURE AS A PHENOMENON OF REFLEXIVE MODERNIZATION IN A RISK SOCIETY: APPLYING ULRICH BECK'S CONCEPTUAL FRAMEWORK

Resume

The paper critically examines cybersecurity culture through the theoretical lens of sociologist Ulrich Beck. Specifically, it engages the theory of reflexive modernization and the concept of the risk society in order to explain cyber risks and cybersecurity culture from a broader sociological perspective. Drawing on relevant academic literature and interpreting cybersecurity issues in light of Beck's theoretical framework, the analysis offers the argument that cybersecurity culture can be understood as a component of the reflexive modernization process, unfolding within the context of a cyber risk society. The risk society in which we live today, alongside numerous other security risks, is to a significant extent characterized by risks arising from technological advancement and the accelerated development of artificial intelligence (AI). Efforts to manage these risks through cybersecurity culture reflect a growing societal awareness of the accompanying adverse effects of modernization. The projection of the future, reflected in the anticipation of catastrophic scenarios in the cyber domain, which requires constant

* E-mail: sladjana.curcic@ies.rs; ORCID: 0000-0001-8276-0983.

preparedness and a proactive approach, is Beck's spirit of reflection, which the cybersecurity culture concept fits well with. The ambivalence inherent in the development of artificial intelligence is inevitably embedded in the nature of cyber risks. Specifically, the simultaneous opportunities and challenges that the advancement of artificial intelligence introduces to the cyber domain generate an intrinsic tension between catastrophe and utopia as competing visions of the future of cybersecurity (Hansen and Nissenbaum 2009). As digital technologies continue to advance, the spectrum of threats will expand, necessitating the continuous adaptation of cybersecurity culture. However, despite the expectation that defense mechanisms against cyber threats will increasingly rely on artificial intelligence, the human factor remains indispensable, as effective cybersecurity ultimately depends on individuals' awareness of the need for protection and their ability to implement appropriate protective strategies, whether AI-based or otherwise. The paper concludes that examining cybersecurity culture through Beck's theoretical framework does not imply its complete explanatory power; it complements existing research efforts aimed at an interdisciplinary understanding of the concept of cybersecurity culture. By positioning the issue of cybersecurity within a primarily sociological framework, widely employed in security studies, this approach contributes to the existing body of research on cybersecurity culture, which has predominantly relied on technically oriented, psychological, and organizational perspectives. Although Beck's theoretical approach has been criticized regarding its ambivalence and conceptual vagueness, this perspective on cybersecurity culture

may serve as an impetus for further research in this field and for continued critical analysis.

Keywords: cybersecurity culture, cyber risks, risk society, reflexive modernization, Ulrich Beck

* Овај рад је примљен 14. јула, а прихваћен за штампу на састанку Редакције 31. августа 2026. године.