

Kibersigurnost ili kibernetička sigurnost kao problem imenovanja i referencijalni jaz u ontologiji sigurnosti

D. Tulić^{*}, R. Fabac[†], D. Delija[‡]

^{*} Sveučilište u Zagrebu, Fakultet organizacije i informatike / Zavod za računarstvo i tehnologiju, Varaždin, Hrvatska

[†] Sveučilište u Zagrebu, Fakultet organizacije i informatike / Zavod za organizaciju, Varaždin, Hrvatska

[‡] Tehničko veleučilište u Zagrebu / Odjel za informacijske i računalne znanosti, Zagreb, Hrvatska
domtulic@foi.hr

Sažetak– Donošenje Zakona o kibernetičkoj sigurnosti u Republici Hrvatskoj potaknulo je raspravu o primjerenosti njegova naziva i njegovu odnosu prema pojmovima kibersigurnosti, informacijske sigurnosti te sigurnosti informacijske i komunikacijske tehnologije (IKT). Kritičari tvrde da kibernetička sigurnost nije jednoznačan prijevod pojma cybersecurity i da ne slijedi uspostavljeni međunarodni referencijalni okvir. U radu se tvrdi da problem nadilazi pitanje prijevoda i odražava dublji nesklad između imenovanja i ontološkog okvira unutar kojega se sigurnost konceptualizira. Oslanjajući se na zakonodavne definicije i Kripkeovu teoriju rigidnih označitelja, rad tvrdi da cybersecurity na međunarodnoj razini funkcionira kao stabilan označitelj, dok kibernetička sigurnost ne nasljeđuje isti referencijalni lanac. Međutim, unutar kibernetičke paradigme i teorije sustava Norberta Wienera, kibernetička sigurnost poprima šire značenje kao sigurnost sociotehničkih sustava upravljanja i komunikacije. Opravdanost naziva Zakona stoga ovisi o prihvaćenom ontološkom okviru.

Ključne riječi– kibernetička sigurnost, kibersigurnost, informacijska sigurnost, kibernetika, sociotehnički sustavi, ontologija sigurnosti, referencijalni jaz, imenovanje

I. UVOD

Izraz kibernetička sigurnost u Hrvatskoj seže do ratifikacije Konvencije o kibernetičkom kriminalu 2002. godine [1]. Od tada se koristi za označavanje pojava koje se u engleskom jeziku nazivaju cybersecurity. Iako se ti izrazi ne podudaraju u potpunosti, a stručne i akademske rasprave bavile su se njihovim pojmovnim razlikovanjem i mogućim prijevodom, te rasprave nisu dovele do bitnih promjena.

Nakon ratifikacije Budimpeštanske konvencije u Hrvatskoj je doneseno više strateških i zakonodavnih dokumenata, među kojima Nacionalna strategija kibernetičke sigurnosti [2] i pripadajući Akcijski plan [3], s ciljem naglašavanja društvene važnosti kibernetičkog prostora. Nadalje, Direktiva (EU) 2022/2555 (NIS2) [4] prenesena je u nacionalno zakonodavstvo Zakonom o kibernetičkoj sigurnosti [5].

Na temelju tih dokumenata i Zakona uspostavljena su posebna državna tijela, uključujući Nacionalni centar za kibernetičku sigurnost u okviru Sigurnosno-obavještajne agencije (SOA), Sektor kibernetičke sigurnosti u Ministarstvu unutarnjih poslova te Zapovjedništvo za kibernetički prostor u Oružanim snagama Republike Hrvatske. Znakovito je da službeni nazivi tih institucija izravno preuzimaju terminologiju Zakona, čime se izraz kibernetička sigurnost institucionalizira unutar nacionalnog sigurnosnog okvira.

Nadalje, izraz kibernetička sigurnost široko se upotrebljava u službenim dokumentima državnih tijela, javne uprave i privatnih organizacija, unatoč očitim nedosljednostima u prijevodu i prevladavajućoj jezičnoj praksi prema kojoj se engleski prefiks cyber- u hrvatskom prenosi kao kiber-, slijedeći grčku fonologiju umjesto zadržavanja engleskog oblika. Posljedično, prefiksi cyber- i kiber- u praksi se pojavljuju kao zamjenjivi.

Rasprave o tim izrazima nisu ograničene na Hrvatsku. Pregled poljskih internetskih medija pokazuje da se slične rasprave vode i unutar poljske sigurnosne zajednice, uključujući razliku između pojmova cyber i cybernetic [6], [7]. Međutim, Direktiva (EU) 2022/2555 (NIS2) prenesena je u poljsko zakonodavstvo pod naslovom Ustawa o Krajowym Systemie Cyberbezpieczeństwa, što doslovno znači Zakon o nacionalnom sustavu kibersigurnosti, pri čemu je zadržan prefiks cyber- umjesto kibernetičke formulacije.

Nadalje, uporaba izraza cybersecurity u Sjedinjenim Američkim Državama kritički je razmatrana u akademskom diskursu. Autori poput Eugenea Spafforda tvrde da prefiks cyber nema dostatnu pojmovnu preciznost i da se često svodi na računal i mreže, čime se zanemaruje njegov širi obuhvat, koji uključuje podatke, procese, ljude, politike, sustave upravljanja i tehnologije u nastajanju, poput robotike i umjetne inteligencije [8].

Važno je da takvo šire razumijevanje već upućuje na sistemski orijentiranu perspektivu u kojoj sigurnost nije ograničena na tehnološke artefakte, nego obuhvaća sociotehničke sustave upravljanja i komunikacije. U tom smislu, kritika pojma cybersecurity ne mora ga nužno potkopavati; ona prije otkriva potrebu za jasnijim ontološkim okvirom, koji se može koherentnije artikulirati unutar kibernetičke tradicije koju je uspostavio Norbert Wiener.

Ako se takvo šire razumijevanje uzme u obzir, izbor terminologije hrvatskog zakonodavca može izgledati manje problematično, a uporaba izraza kibernetička sigurnost može se smatrati pojmovno obranjivom unutar proširenog, sistemski orijentiranog okvira.

Ostatak rada strukturiran je na sljedeći način. Drugo poglavlje iznosi definicije kiber/kibernetičke sigurnosti, informacijske sigurnosti, IKT sigurnosti i sigurnosti kao takve, zajedno s njihovim međusobnim odnosima. Treće poglavlje analizira problem imenovanja primjenom teorije rigidnih označitelja američkog logičara i filozofa Saula Kripkea. Četvrto poglavlje razvija autorsko tumačenje kibernetičke sigurnosti unutar teorije sustava i kibernetičke znanosti koju je utemeljio Norbert Wiener. Peto poglavlje zaključuje raspravu, nakon čega slijedi popis literature.

Kako bi se ova pitanja obradila na strukturiran način, rad primjenjuje konceptualnu i analitičku metodologiju usmjerenu na ispitivanje odnosa između imenovanja, značenja i referencije u sigurnosnoj terminologiji. Konceptualno razjašnjenje ključnih pojmova povezuje se s komparativnom analizom njihove uporabe u zakonodavnim dokumentima, međunarodnim normama i akademskoj literaturi. Analiza se dodatno temelji na primjeni Kripkeove teorije rigidnih označitelja i elemenata kibernetičke teorije sustava.

II. KONCEPTUALNE DEFINICIJE I NJIHOVI MEĐUODNOSI

U znanosti i praksi definicije su ključne kako bi se utvrdilo raspravlja li se o istim pojmovima te kako bi se uspostavile primjerene metrike za procjenu učinkovitosti primijenjenih kontrola.

U mnogim publikacijama, osobito uvodnima, kiber/kibernetička sigurnost i informacijska sigurnost često se tretiraju kao pojmovni sinonimi, dok se sigurnost informacijske i komunikacijske tehnologije (IKT) promatra isključivo kao tehnološka domena i rijetko se razmatra samostalno.

A. Informacijska sigurnost

Norma HRN EN ISO/IEC 27000:2020 definira informacijsku sigurnost kao očuvanje povjerljivosti, cjelovitosti i raspoloživosti informacija [9]. Prema HRN EN ISO/IEC 27002:2022, informacije mogu biti stvorene, prikupljene, obrađene, pohranjene, prenesene ili prikazane u različitim oblicima - elektroničkom, fizičkom ili usmenom - unutar organizacija svih vrsta i veličina [10].

Hrvatski Zakon o informacijskoj sigurnosti definira informacijsku sigurnost kao stanje povjerljivosti, cjelovitosti i raspoloživosti ostvareno propisanim mjerama, normama i organizacijskom potporom [11]. Nadalje, informacijski sustav definira kao komunikacijski, računalni ili elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose radi osiguravanja raspoloživosti ovlaštenim korisnicima. Obje se definicije oslanjaju na model CIA.

Whitman i Mattord, međutim, informacijsku sigurnost definiraju šire, kao zaštitu informacija i njihovih kritičnih elemenata, uključujući sustave, sklopovlje, pohranu i mehanizme prijenosa koji ih podupiru [12].

B. Sigurnost informacijske i komunikacijske tehnologije (IKT)

Suvremeni europski zakonodavni i normativni dokumenti ne daju izričitu definiciju IKT sigurnosti. Posljednja formalna definicija nalazi se u normi ISO/IEC 13335-1, koja IKT sigurnost definira kao skup svih aspekata povezanih s postizanjem i održavanjem povjerljivosti, cjelovitosti, raspoloživosti, neporecivosti, odgovornosti, autentikacije i pouzdanosti informacijskih resursa [13].

Iako je ta norma u međuvremenu povučena, postavila je temelje suvremenim sustavima upravljanja informacijskom sigurnošću (ISMS). Danas se IKT sigurnost implicitno obrađuje unutar porodice normi ISO/IEC 27000 i zakonodavstva EU-a kroz zaštitu mrežnih i informacijskih sustava. Posljedično, IKT sigurnost rijetko se definira samostalno.

U tom smislu IKT sigurnost može se razumjeti kao područje usmjereno na zaštitu tehnološke infrastrukture koja omogućuje pohranu, obradu i prijenos informacija, neovisno o njihovu sadržaju ili značenju.

C. Kibernetika / kibernetska sigurnost

Prije prikaza suvremenih definicija potrebno je razjasniti podrijetlo pojma. Prefiks cyber potječe od kibernetike, znanosti o upravljanju i komunikaciji u životinja i strojeva, koju je utemeljio američki znanstvenik Norbert Wiener [14]. Sam pojam potječe od grčke riječi *kybernetes*, koja znači kormilar ili upravljač.

Kibernetika, kao pojam uveden 1947. godine, nastojala je objediniti teoriju komunikacije, teoriju upravljanja i statističku mehaniku u koherentan znanstveni okvir. Iako je poslije izgubila status samostalne discipline i integrirala se u opću teoriju sustava, njezin je utjecaj opstao, osobito u računalnim znanostima.

Prefiks cyber ponovno je stekao kulturnu prepoznatljivost romanom *Neuromancer* Williama Gibsona, koji je uveo kibernetički prostor kao „konsenzualnu halucinaciju“. I Gibsonova fikcionalna vizija i Wienerova radikalna koncepcija kibernetičkog organizma - potencijalno svodivog na čisti informacijski obrazac - pridonijele su novoj ontologiji subjekta, u kojoj identitet nije nužno vezan uz materijalni supstrat, nego uz informacijsku strukturu [15].

Prefiks cyber stekao je intelektualnu i kulturnu vidljivost i u djelima poljskog pisca i mislioca Stanisława Lema, koji je često upotrebljavao pojam kibernetike (*kibernetyka/cybernetyka*) i povezane koncepte u svojoj prozi i esejima. U djelu *Dialogi* [16] kibernetika čini središnji tematski okvir, dok se u romanima poput *Edena* [17] i *Cyberjade* [18] izričito pojavljuje lik „kibernetičara“.

¹ Dvostruka uporaba izraza cyber i cybernetic u ovom radu namjerna je. Ona odražava terminološku neodređenost prisutnu u hrvatskom stručnom i zakonodavnom diskursu, u kojem se oba oblika pojavljuju paralelno

i često se koriste zamjenjivo unatoč različitim povijesnom i konceptualnom podrijetlu.

U djelu Summa Technologiae [19] Lem se izravno bavi kibernetičkim pojmovima poput povratne veze, homeostaze i modeliranja sustava, ugrađujući ih u šire promišljanje tehnološke evolucije. Čak i kada su političke okolnosti privremeno zahtijevale terminološki oprez, konceptualna usmjerenost prema kibernetici ostala je očita.

Unutar takva proširenog razumijevanja nastale su brojne izvedenice: cybercrime, cyberattack, cyberculture, cyberespionage, cyberterrorism, cyberrisk, cyberresilience, cyberactivism, cybersociety, cyberbody, cyberfeminism, cyberpsychology i druge. Samo u engleskom jeziku više od 150 izraza koristi taj prefiks.

Prva zabilježena strateška uporaba prefiksa pojavila se u američkom vojnom diskursu, osobito u članku „Cyberwar Is Coming“ Johna Arquille i Davida Ronfeldta [20]. Izraz je poslije populariziran u kontekstu javnih politika, među ostalim i zahvaljujući Michaelu Vatisu, koji ga je, prema navodima, prihvatio kako bi privukao pozornost kreatora politika [21].

Stoga kiber/kibernetička sigurnost nije nastala isključivo kao tehnički odgovor na računalne prijetnje, nego kao dio širega konceptualnog pomaka u razumijevanju sustava, informacija i identiteta.

U suvremenom zakonodavstvu i normama postoje brojne definicije kiber/kibernetičke sigurnosti. Hrvatski Zakon o kibernetičkoj sigurnosti preuzima definiciju iz Uredbe (EU) 2019/881 [22], prema kojoj kibersigurnost obuhvaća aktivnosti potrebne za zaštitu mrežnih i informacijskih sustava, njihovih korisnika i drugih pogođenih osoba od kiberprijetnji. Znakovito je da hrvatski zakon koristi izraz kibernetička sigurnost, dok se u dokumentima EU-a prevedenima na hrvatski upotrebljava izraz kibersigurnost, što otkriva terminološku nedosljednost.

Američki Nacionalni institut za standarde i tehnologiju (NIST) definira kibersigurnost kao sprječavanje oštećenja, zaštitu i obnovu računalnih sustava i elektroničkih komunikacija, uključujući osiguravanje raspoloživosti, cjelovitosti, autentikacije, povjerljivosti i neporecivosti [23].

Uz zakonodavne i stručne definicije razvijene su i strukturirane taksonomije radi definiranja i sistematiziranja kibersigurnosti i povezanih pojmova. Primjerice, taksonomija VOUND daje definicije kibersigurnosti i niza povezanih izraza, nudeći strukturirani konceptualni okvir za razumijevanje područja [24]. Znakovito je da se u hrvatskom kontekstu u taksonomiji VOUND prihvaća izraz kibernetička sigurnost, što dodatno ilustrira lokalizaciju terminologije i njezino odstupanje od dominantne međunarodne uporabe. Razlike u terminologiji i konceptualnom obuhvatu među različitim kontekstima i izvorima sustavno su prikazane u Tablici I.

Iz tih definicija, povijesnog razvoja i suvremene uporabe postaje razvidno da se problem kibernetičke sigurnosti ne iscrpljuje u prijevodu ili terminološkoj dosljednosti. Umjesto toga, riječ je o dubljem odnosu između imena, značenja i referencije. Stoga sljedeće poglavlje problem imenovanja razmatra u okviru filozofije jezika, oslanjajući se na teoriju rigidnih označitelja Saula Kripkea.

TABLICA I. USPOREDNA UPORABA TERMINOLOGIJE POVEZANE SA SIGURNOŠĆU

Kontekst/izvor	Upotrijebljeni izraz	Opseg definicije
EU (Uredba 2019/881)	Kibersigurnost	Zaštita mrežnih i informacijskih sustava, korisnika i povezanih subjekata
Hrvatska (Zakon o kibernetičkoj sigurnosti)	Kibernetička sigurnost	Područje ekvivalentno kibersigurnosti, izraženo drukčijom terminologijom
SAD (NIST)	Kibersigurnost	Zaštita, prevencija i oporavak računalnih sustava i komunikacija
ISO/IEC 27000	Informacijska sigurnost	Očuvanje povjerljivosti, cjelovitosti i raspoloživosti (CIA)
Taksonomija VOUND (CERT.hr)	Kibernetička sigurnost	Strukturirani skup povezanih pojmova i domena unutar kibersigurnosti s definicijama

III. ESENCIJALIZAM I RIGIDNO OZNAČAVANJE U IMENOVANJU KIBERSIGURNOSTI

Pri razmatranju izraza kibernetička sigurnost kako se pojavljuje u naslovu hrvatskog Zakona nije dovoljno odbaciti problem kao puki pogrešan prijevod engleskog izraza cybersecurity. Problem je konceptualno složeniji i može se analizirati kroz djelo američkog filozofa Saula Kripkea.

U djelu Imenovanje i nužnost Kripke u svojoj kritici deskriptivne teorije značenja uvodi pojam rigidnog označitelja [25]. Rigidni označitelj upućuje na isti objekt u svim mogućim svjetovima u kojima taj objekt postoji, neovisno o njegovim kontingentnim svojstvima. Iako cybersecurity nije rigidni označitelj u strogom Kripkeovu smislu - koji se ponajprije primjenjuje na vlastita imena i prirodne vrste - može se razmatrati analogijskom primjenom rigidnog označavanja, osobito u odnosu na fiksiranje i prijenos referencije unutar jezične zajednice.

Prema Kripkeovu prikazu, referencija se fiksira početnim činom imenovanja - koji se metaforički često opisuje kao „krštenje“ - a zatim se prenosi referencijalnim lancem. Unutar tog okvira esencijalna svojstva razlikuju se od kontingentnih opisa, čime se dopušta mogućnost da entiteti posjeduju nužna obilježja koja konstituiraju njihov identitet.

Taj teorijski okvir omogućuje preciznije razumijevanje problema imenovanja u slučaju pojma cybersecurity. Unutar međunarodne stručne i akademske zajednice izraz cybersecurity funkcionira kao stabilan označitelj, dosljedno upućujući na relativno dobro definiran skup praksi, znanja i institucionalnih aranžmana usmjerenih na zaštitu umreženih informacijskih sustava od namjernih digitalnih prijetnji. Njegova je referencija stabilizirana dugotrajnom uporabom u znanstvenom, industrijskom i normativnom kontekstu.

Nasuprot tomu, hrvatski izraz kibernetička sigurnost ne nasljeđuje uspješno stabiliziranu referencijalnu funkciju povezanu s pojmom cybersecurity. On se pojavljuje kao deskriptivni izraz čija etimologija i povijesne asocijacije upućuju na šire područje kibernetike kako ju je izvorno formulirao Norbert Wiener. Time nastaje referencijalni jaz: naziv zakona nastoji rigidno označiti fenomen koji je međunarodno poznat kao cybersecurity, dok odabrani izraz priziva drukčiju konceptualnu tradiciju.

Problem se može razmotriti i u esencijalističkim pojmovima. Esencijalna domena kibersigurnosti odnosi se na zaštitu umreženih informacijskih sustava, podataka i digitalnih infrastruktura od zlonamjernog djelovanja. Esencijalna domena kibernetike, međutim, obuhvaća teoriju upravljanja, komunikacije i povratne veze u biološkim i mehaničkim sustavima. Kada zakonodavni akt namijenjen uređivanju prvoga područja prihvati terminologiju povijesno povezanu s drugim, na razini biti nastaje konceptualni nesklad.

Iz Kripkeove perspektive dodatna poteškoća leži u pokušaju lokalnog „krštenja“. Umjesto preuzimanja već stabiliziranoga referencijalnog lanca, zakonodavac kao da uvodi novog kandidata za rigidno označavanje. Međutim, budući da izraz kibernetička sigurnost u jeziku već nosi uspostavljene semantičke asocijacije, njegova sposobnost da uspješno fiksira referenciju na namjeravani fenomen ostaje predmet prijepora unutar stručne zajednice.

Naposlijetku, Kripkeovo razlikovanje nužnih i kontingentnih istina pojašnjava da je izbor terminologije za zakonodavni akt kontingentna odluka. Nijedan normativni akt ne može retroaktivno promijeniti uspostavljeni referencijalni lanac unutar međunarodne epistemičke zajednice. Kritika koju iznose dijelovi stručne javnosti stoga se može tumačiti kao intuitivno prepoznavanje filozofske napetosti između imena, značenja i referencije.

IV. KIBERNETIČKA SIGURNOST U OKVIRU SOCIOTEHNIČKIH SUSTAVA

Nakon analize problema imenovanja i referencijalnog jaza utvrđenog u prethodnom poglavlju, u ovom se odjeljku razmatra može li pojam kibernetičke sigurnosti steći konceptualnu koherentnost ako se shvati kao sigurnost kibernetičkih sustava.

U djelu Kibernetika ili upravljanje i komunikacija u životinji i stroju Norbert Wiener formulirao je kibernetiku kao znanost o upravljanju i komunikaciji primjenjivu podjednako na biološke organizme i strojeve. U svojem povijesnom prikazu automata Wiener prepoznaje odlučujući pomak - od mehaničke snage prema komunikacijskom inženjerstvu - pri kojem precizan prijenos i regulacija signala postaju središnji. Taj pomak označuje prijelaz od inženjerstva usmjerenog na energiju prema regulaciji sustava usmjerenoj na informacije.

Presudno je da Wiener ne uspostavlja strogu ontološku granicu između ljudi i strojeva. I jedni i drugi promatraju se kao sustavi kojima upravljaju poruke, šum, tok informacija, tehnike kodiranja, povratna veza i homeostaza. Takvi sustavi postoje, kako Wiener tvrdi, kako bi regulatornim mehanizmima stvarali lokalne i privremene preokrete entropije. Iz te perspektive stabilnost nije statičko svojstvo, nego trajan proces informacijske regulacije.

Sigurnost se unutar kibernetičkog okvira stoga može tumačiti ne samo kao zaštita pojedinačnih komponenti ili podataka, nego kao očuvanje systemske stabilnosti u uvjetima poremećaja. Povratna veza djeluje kao regulatorni mehanizam koji neprekidno prilagođava odnose između unutarnjeg i vanjskog okruženja, održavajući homeostazu obradom informacija i prilagodljivim odgovorom. Kibernetički je sustav siguran u mjeri u kojoj ostaje upravljiv, otporan i sposoban održavati strukturu koherentnost unatoč šumu, poremećajima ili neprijateljskom djelovanju.

Takvo razumijevanje podudara se sa širim promišljanjima složenih tehnoloških sustava, uključujući ona koja naglašavaju autonomiju, emergenciju i moguć gubitak upravljivosti u velikim infrastrukturnim sustavima. Kada sustavi evoluiraju izvan centraliziranog upravljanja, sigurnost se ne može svesti na obranu perimetra ili izolirane zaštitne mjere; ona postaje pitanje upravljanja dinamičkim interakcijama unutar distribuiranih sociotehničkih okruženja.

U tom smislu pojam kibernetičke sigurnosti proširuje područje tradicionalno povezano s informacijskom ili IKT sigurnošću. Obuhvaća ne samo tehničke artefakte i digitalne infrastrukture, nego i ljudske operatore, organizacijske strukture i procese odlučivanja ugrađene u njih. Sigurnost postaje systemsko svojstvo koje nastaje iz interakcije tehnoloških i društvenih sastavnica.

Promatran u svjetlu prethodnog poglavlja, ovaj okvir sugerira moguće razrješenje referencijalnog jaza. Premda zakonodavni izraz kibernetička sigurnost možda ne nasljeđuje stabilizirani referencijalni lanac povezan s pojmom cybersecurity, ipak može steći konceptualnu legitimnost unutar šire kibernetičke ontologije. Ako se sigurnost razumije kao regulacija i stabilizacija sociotehničkih sustava kojima upravljaju informacije i povratne veze, izraz kibernetička sigurnost nije konceptualno pogrešno smješten, nego normativno ambiciozan.

Stoga opravdanost naziva Zakona u konačnici ovisi o prihvaćenom ontološkom okviru. Unutar uskog tehnološkog razumijevanja naziv se čini neusklađenim s međunarodnom uporabom. Unutar perspektive kibernetičkih sustava, međutim, može se tumačiti kao pokušaj artikuliranja obuhvatnijeg modela sigurnosti - modela koji integrira upravljanje, komunikaciju i systemsku otpornost.

V. ZAKLJUČAK

Analiza je pokazala da problem imenovanja Zakona o kibernetičkoj sigurnosti ne proizlazi iz jednostavnoga pogrešnog prijevoda pojma cybersecurity, nego iz dubljega referencijalnog i ontološkog nesklada. Unutar međunarodnoga stručnog diskursa izraz cybersecurity funkcionira kao stabilan označitelj koji upućuje na jasno definiran skup praksi i pojmova povezanih sa zaštitom mrežnih i informacijskih sustava. U tom smislu izraz kibernetička sigurnost ne slijedi uspostavljeni referencijalni lanac i može stvarati terminološku nepreciznost.

Međutim, kada se fenomen sigurnosti razmatra unutar okvira kibernetike i teorije sustava, pojam kibernetičke sigurnosti poprima šire i konceptualno koherentnije značenje. U takvu pristupu sigurnost se ne odnosi isključivo na tehnologiju ili informacije, nego na sociotehničke sustave upravljanja i komunikacije kao cjelinu. Iz te perspektive naziv Zakona ne predstavlja pogrešku; naprotiv, implicitno upućuje na šire razumijevanje sigurnosti koje nadilazi usko tehničko poimanje.

Stoga se može zaključiti da je spor oko imenovanja istodobno i spor oko ontološkog okvira unutar kojega se sigurnost razumije. Ako se prihvati uži, tehnološki okvir, naziv Zakona djeluje terminološki problematično. Ako se, međutim, prihvati kibernetički svjetonazor, imenovanje postaje konceptualno opravdano.

Kontroverza oko imenovanja tako ne otkriva samo jezično neslaganje, nego i dublju filozofsku napetost između uspostavljenih referencijalnih praksi i konkurentskih ontoloških okvira za razumijevanje sigurnosti u suvremenim sociotehničkim sustavima.

LITERATURA

- [1] Vijeće Europe, Convention on Cybercrime, ETS br. 185, Budimpešta, Mađarska, 23. studenoga 2001. Pristupljeno: 20.12.2025. [Mrežno]. Dostupno: <https://rm.coe.int/1680081561>
- [2] Vlada Republike Hrvatske, Nacionalna strategija kibernetičke sigurnosti, Zagreb, Hrvatska, 2015. Pristupljeno: 20.12.2025. [Mrežno]. Dostupno: https://mup.gov.hr/UserDocsImages/ministarstvo/kibernetika/strategija_kibernetika.pdf
- [3] Ured Vijeća za nacionalnu sigurnost Republike Hrvatske, Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti, Zagreb, Hrvatska, 2015. Pristupljeno: 20.12.2025. [Mrežno]. Dostupno: [https://www.uvns.hr/UserDocsImages/dokumenti/Akcijski%20plan%20za%20provedbu%20Nacionalne%20strategije%20kiberneticke%20sigurnosti%20\(2015.\).pdf](https://www.uvns.hr/UserDocsImages/dokumenti/Akcijski%20plan%20za%20provedbu%20Nacionalne%20strategije%20kiberneticke%20sigurnosti%20(2015.).pdf)
- [4] Europski parlament i Vijeće Europske unije, Direktiva (EU) 2022/2555 od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, Službeni list Europske unije, 2022. Pristupljeno: 20.10.2025. [Mrežno]. Dostupno: <https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32022L2555>
- [5] Hrvatski sabor, Zakon o kibernetičkoj sigurnosti, Narodne novine br. 14/24, 2024.
- [6] M. Świetlińska, "Cyberbezpieczeństwo czy bezpieczeństwo cybernetyczne?", pristupljeno: 20.10.2025. [Mrežno]. Dostupno: <https://www.securitymagazine.pl/pl/a/cyberbezpieczenstwo-czy-bezpieczenstwo-cybernetyczne>
- [7] Orange Polska, "Bezpieczeństwo cybernetyczne," pristupljeno: 20.10.2025. [Mrežno]. Dostupno: <https://www.orange.pl/poradnik-dla-firm/cyberbezpieczenstwo/bezpieczenstwo-cybernetyczne/>
- [8] E. H. Spafford, L. Metcalf i J. Dykstra, Cybersecurity myths and misconceptions: Avoiding the pitfalls and breaking through the hype, Boston, MA, SAD: Pearson Education, 2023.
- [9] Hrvatski zavod za norme, HRN EN ISO/IEC 27000:2020, Informacijska tehnologija - Sigurnosne tehnike - Sustavi upravljanja informacijskom sigurnošću - Pregled i rječnik, 2020.
- [10] Hrvatski zavod za norme, HRN EN ISO/IEC 27002:2022, Informacijska sigurnost, kibersigurnost i zaštita privatnosti - Kontrole informacijske sigurnosti, 2022.
- [11] Republika Hrvatska, Zakon o informacijskoj sigurnosti, Narodne novine, br. 79/07, 2007.
- [12] M. E. Whitman i H. J. Mattord, Principles of information security, Boston, MA, Thomson Course Technology, 2009.

- [13] International Organization for Standardization, ISO/IEC 13335-1:2004, Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models, 2004.
- [14] N. Wiener, Cybernetics: Or Control and Communication in the Animal and the Machine, Pariz, Francuska: Hermann & Cie; Cambridge, MA, SAD: MIT Press, 1948.
- [15] D. Tomas, "Feedback and cybernetics," Theory, Culture & Society, sv. 12, br. 3, str. 105-121, 1995.
- [16] S. Lem, Dialogi, Krakov, Poljska: Wydawnictwo Literackie, 1957.
- [17] S. Lem, Eden, Krakov, Poljska: Wydawnictwo Literackie, 1959.
- [18] S. Lem, Cyberiada, Krakov, Poljska: Wydawnictwo Literackie, 1965.
- [19] S. Lem, Summa Technologiae, Krakov, Poljska: Wydawnictwo Literackie, 1964.
- [20] J. Arquilla i D. Ronfeldt, "Cyberwar is coming!," Comparative Strategy, sv. 12, br. 2, str. 141-165, 1993.
- [21] F. Kaplan, Dark Territory: The Secret History of Cyber War, New York, NY, SAD: Simon & Schuster, 2016.
- [22] Europski parlament i Vijeće Europske unije, Uredba (EU) 2019/881 od 17. travnja 2019. (Akt o kibersigurnosti), Službeni list Europske unije, 2019. Pristupljeno: 20.12.2025. [Mrežno]. Dostupno: <https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32019R0881>
- [23] National Institute of Standards and Technology, "Cybersecurity," NIST Computer Security Resource Center Glossary, pristupljeno: 20.12.2025. [Mrežno]. Dostupno: <https://csrc.nist.gov/glossary/term/cybersecurity>.
- [24] CERT.hr, Nacionalna taksonomija računalno-sigurnosnih incidenata, Hrvatski nacionalni CERT, 2021. Pristupljeno: 10.04.2026. [Mrežno]. Dostupno: <https://www.cert.hr/wpcontent/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf>
- [25] S. Kripke, Imenovanje i nužnost, Zagreb, Hrvatska: KruZak, 1997.