Nenad Pandurević[1]

DOI10.7251/ZJF2514319P

EKONOMIJA DIGITALNE BEZBJEDNOSTI

Apstrakt: Kako digitalizacija postaje ključna za funkcionisanje privrede i društva tako i pitanje bezbjednosti u digitalnom svijetu dobija na ekstremnoj važnosti. Pitanje digitalne bezbjednosti godinama se posmatralo isključivo kao tehničko pitanje. Zaštitom podataka, informacija, mreža, kanala komuniciranja i sl. bavili su se informatički eksperti i privatni sektor. Sa rastućom digitalizacijom tržište digitalne bezbjednosti narasta do neslućenih razmjera. Međutim, uprkos ogromnim ulaganjima u borbu protvi sajberkriminala, svi subjekti na tržištu suočavaju se i dalje sa rastućim rizicima i šetama.

Ekonomisti uočavaju da prepustan samo privatnoj inicijativi i ekspertskim rješenjima prijetnje po digitalnu bezbjednost neće biti ukolnjene. Naime, prepoznaje se da proizvodi i usluge na tržištu digitalne bezbjednopsti imaju sve one osobine koje neoklasična ekonomija prepozanje kao razlog za tržišni neuspjeh. Digitalna bezbednost nije samo tehnički problem, već i složeno ekonomsko pitanje vođeno podsticajima, eksternalijama i dinamikom tržišta. Efikasna rješenja zahtijevaju kombinaciju tehničkih mjera, vladine intervencije, ekonomskih poticaja za rješavanje tržišnih neuspjeha, usklađivanje interesa zainteresovanih učesnika i podsticanje globalne saradnje.

Ključne riječi: Digitalni prostor, digitalna bezbjednost, ekonomija digitalne bezbjednosti, neuspjeh tržišta, politike digitalne bezbjednosti

THE ECONOMICS OF CYBERSECURITY

Abstract: As digitalization becomes a cornerstone of economic and societal functions, the importance of security in the digital realm is rapidly escalating. Historically, cybersecurity has been treated primarily as a technical issue, with IT experts and the private sector focusing on safeguarding data, information, networks, and communication channels. The increasing pace of digitalization has propelled the cybersecurity market to unprecedented growth. Yet, despite substantial investments in combating cybercrime, market participants continue to face escalating risks and challenges.

Economists argue that relying solely on private initiatives and technical solutions is insufficient to achieve significant improvements in cybersecurity. Cybersecurity products and services exhibit characteristics commonly associated with market failures, as identified by neoclassical economics. This indicates that cybersecurity is not merely a technical concern, but a multifaceted economic issue influenced by incentives, externalities, and market forces. Addressing these challenges requires an integrated approach, combining technical measures, policy interventions, and economic incentives to mitigate market failures, align stakeholder interests, and promote global cooperation.

Keywords: Cyberspace, cybersecurity, cybersecurity economics, market failure, cybersecurity policies

1 Parlamentarna skupština Bosne i Hercegovine, nenadp@gmail.com

1. UVOD

Procjenjuje se da će ekonomija koja se povezuje sa kriminalnim napadima u sajber[1] prostoru u 2024. godini iznositi 9,5 hiljada milijardi američkih dolara, po čemu je to treća svjetska ekonomija, iza SAD i Kine.[2] Ono što je još značajnije jeste to što ekonomija povezana sa sajber napadima ekspandira u svim svojim segmentima i to značajnim stopama rasta. Prosječna šteta koju pogođeni subjekti trpe je oko 5 miliona dolara po jednom napadu i u 2024. je 11% viša nego godinu dana ranije. Svi troškovi povezani sa sajber napadima, kao što su troškovi gubitaka u poslovanju, troškovi otkrivanja napada, troškovi oporavka sistema i slično, takođe, bilježe rast iz godine u godinu (*IBM, 2024*). Između 2014. i 2023. godine, broj prijavljenih sajber incidenata u svijetu rastao je prosječnom godišnjom stopom od 21%, sa medijanom od 31%. Očekuje se da će se ovaj uzlazni trend nastaviti, posebno u zemljama u razvoju, prije svega zbog visoke stope digitalizacije, niže političke i ekonomske stabilnosti i nedovoljnih mjera digitalne bezbjednosti (*Cobos, 2024*).

Rizik od sajber napada se ubrzano povećava uporedo sa ubrzanim rastom digitalizacije. Sve veće oslanjanje na digitalne sisteme za lične, profesionalne i vladine operacije proširuje područja izloženosti opasnosti od napada sajber kriminalaca. Porast uređaja „interneta stvari" (*IoT - Internet of Things*), računarstva u oblaku i mobilne tehnologije stvara nove ranjivosti. Tako npr. broj uređaja „interneta stvari" je povećan sa 800 miliona u 2010. na 25 milijardi 2024., sa projekcijom do 30 milijardi u 2025..[3] Opasnosti koje to donosi kreću se od nesvjesnog špijuniranja ili kompromitovanja podataka pa do nemogućnosti zaključavanja vlastitog doma. Korisnici mogu čak postati dio *botneta* koji napada internet. Nesigurna veb kamera – zajedno s milionima drugih – mogla bi se koristiti za napad na električnu mrežu cijele zemlje. Sličnu ekspanziju doživljava i „tehnologija u oblaku". I dok se generalno smatra da *cloud* tehnologija poboljšava digitalnu bezbjednost, ona istovremeno predstavlja veoma značajne izdatke za kompanije[4], dok rizik, iako nešto niži i dalje postoji. Istovremeno širenje kriptovaluta olakšavaj anonimne transakcije, olakšavajući sajber kriminalcima da traže i primaju isplate otkupnine bez straha od otkrivanja.

Problem digitalne bezbjednosti dodatno komplikuje rastući nedostatak radne snage kvalifikovane za ovu oblast. Prema izvještaju IBM u 2024. godini čak 53% ispitanih kompanija je prijavilo problem nedostatka kvalifikovanog osoblja, što je povećanje od 26% u odnosu na prethodnu godinu. Rješenja se nastoje pronaći upotrebom vještačke inteligencije, ali to dodatno podiže troškove i ne eliminiše rizike od sajber napada (*IBM, 2024*). Procjenjuje se da je u 2023. godini u svijetu nedostajalo preko 4 miliona stručnjaka za sajber bezbjednost (*Cobos, 2024, 76*).

1 Izrazi *digitalni, sajber i kibernetički* u ovom radu se koriste kao sinonimi.
2 https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger
3 https://www.statista.com/topics/2637/internet-of-things/
4 https://www.forbes.com/councils/forbestechcouncil/2023/05/08/the-hidden-costs-of-cybersecurity/

2. PROBLEM

Problem o kojem govorimo u ovom radu tiče se nedovoljnog razumijevanja ekonomskog aspekta digitalne bezbjednosti. To nerazumijevanje jednako se odnosi na pojedince, kompanije i vladin sektor. Proizvodi i usluge na tržištu digitalne bezbjednosti ispoljavaju skoro sve karakteristike tipične za slučaj otkazivanja tržišta. To za rezultat ima neadekvatnu valorizaciju rizika, te shodno tome, neefikasnost u investiranju i uopšte u borbi protiv sajber kriminala.

O nedovoljnom razumijevanju ekonomskih karakteristika digitalne bezbjednosti govori i podatak da čak preko 40% sajber incidenata ostane neobjavljeno od strane napadnute firme (*Cobos, 2024, 49*) jer objavljivanje takvih podataka može značajno narušiti reputaciju firme u očima kupaca, akcionara, javnosti, zaposlenih... . Dalje, firme ili pojedinci su često pogođeni putem trećih učesnika na tržištu (provajdera) pri čemu malo mogu uticati na vlastitu bezbjednost ili pak firme koje investiraju u vlastitu bezbjednost često ne mogu pokupiti sve koristi od svojih ulaganja (pozitivne eksternalije). Istovremeno ukupni društveni troškovi su ogromni. Sajber incidenti mogu uticati na makroekonomsku stabilnost zemlje, čak su zabilježeni slučajevi smanjenja BDP za 2,4%. Sajber bezbjednost je ključna za inkluzivan i održiv rast nacija. Određene procjene ukazuju da zemlja u razvoju smanjenjem sajber napada mogu povećati vlastiti BDP i do 1,5%. (*Cobos, 2024, 50)*.

Slika 1. Dilema zatvorenika u slučaju ulaganja u digitalnu bezbjednost

		KOMPANIJA B	
		Bezbjedna	Nebezbjedna
KOMPANIJA A	Bezbjedna	40, 40	25, 50
	Nebezbjedna	50, 25	30, 30

Izvor: Kelly, 2017, 522.

U radu iz 2017. godine, "Ekonomija sajber bezbjednosti", David Kelly (*Kelly, 2017, 522*) raspravlja o primjeni dileme zatvorenika na odluke o ulaganju u digitalnu bezbjednost. Zatvorenikova dilema je fundamentalni koncept u teoriji igara koji ilustruje zašto dvije racionalne osobe možda ne sarađuju, čak i ako je to u njihovom najboljem interesu. U kontekstu digitalne bezbjednosti, ova dilema se manifestuje kada organizacije moraju odlučiti da li da investiraju u mjere digitalne bezbjednosti. Na slici 1 imamo primjer dvije kompanije, A i B, od kojih se svaka suočava sa izborom da investira u digitalnu bezbjednost („sarađuje") ili ne („ne sarađuje"). Ako obje

kompanije investiraju, one poboljšavaju svoju bezbjednost i doprinose bezbjednijem cjelokupnom digitalnom okruženju, od čega će obje imati koristi, ako nijedna ne investira, obje ostaju ranjive na sajber prijetnje. Međutim, ako jedna ulaže, a druga ne, kompanija koja ne investira može imati koristi od bezbjednosnih mjera kompanije koja investira, a da pritom ne snosi troškove. Dakle, dok uzajamno ulaganje vodi do najboljeg zajedničkog ishoda, iskušenje besplatnog korištenja može dovesti do toga da obje kompanije premalo ulažu u digitalnu bezbjednost. Ovo nedovoljno ulaganje može rezultirati većim ranjivostima i većim troškovima potencijalnih sajber napada. Ova analiza naglašava važnost razumijevanja ovih ekonomskih podsticaja za razvoj strategija koje podstiču adekvatna ulaganja u digitalnu bezbjednost u svim organizacijama.

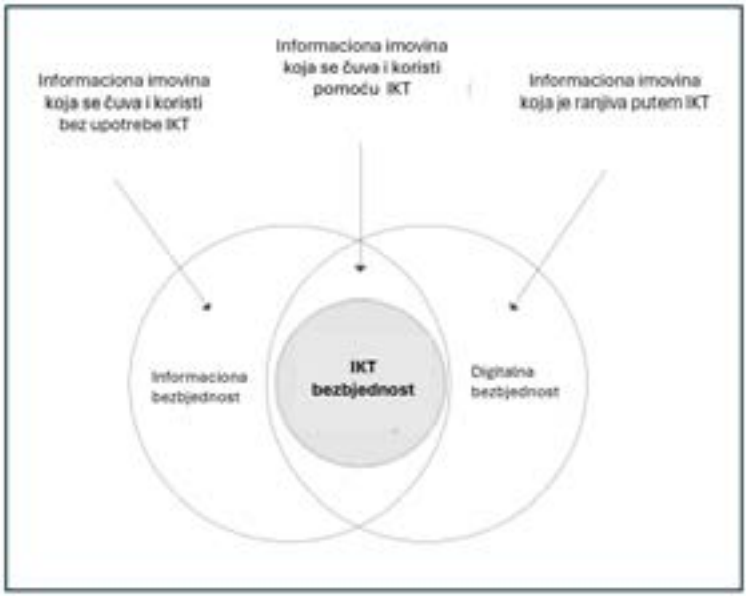
Dakle, glavni problem ekonomije digitalne bezbjednosti može se definisati kao neusklađenost podsticaja među ključnim akterima na tržištu, što dovodi do nedovoljnog ulaganja u mjere bezbjednosti i neefikasne raspodjele rizika i troškova. To rezultira sistemskim ranjivostima, gdje napadači iskorištavaju slabe karike u digitalnom ekosistemu, uzrokujući široku ekonomsku i društvenu štetu. Rješavanje ovih izazova zahtijeva mješavinu tržišnih podsticaja, propisa i tehnoloških inovacija.

3. TERMINOLOGIJA

Ekonomija digitalne bezbjednosti, kao oblast ekonomskog istraživanja novijeg je datuma, još uvijek je u fazi svog terminološkog i metodološkog uobličavanja. Istovremeno obuhvata dvije veoma široke oblasti istraživanja: digitalnu bezbjednost i ekonomiju, kao dva potpuno odvojena istraživačka područja, koja su predmet istraživanja potpuno nezavisnih istraživača, informatičara i ekonomista.

Radi definisanja i razumijevanja ekonomije digitalne bezbjednosti, poželjno je imati što je moguće jasniju definiciju same digitalne bezbjednosti. U tom smislu postoji mnogo definicija pojma digitalna ili sajber bezbjednost (koji se uglavnom upotrebljavaju kao sinonimi) i uglavnom se one prepliću sa definicijama informacione i IKT bezbjednosti. Informaciona bezbjednost se odnosi na zaštitu ukupne imovine u formi informacija bez obzira na to gdje se ona nalazi i na koji način se komunicira. Dakle, informaciona bezbjednost se proširuje na IKT bezbjednost u cilju zaštite samih informacija, bez obzira na njihov trenutni oblik ili lokaciju, dok se digitalna bezbjednost treba posmatrati kao proširenje informacione bezbjednosti. Digitalna bezbjednost bi trebalo da se odnosi na zaštitu više od same zaštite informacija ili informacionih sistema. Digitalna bezbjednost se takođe odnosi na zaštitu osoba koje koriste resurse u digitalnom okruženju i oko njega, zaštitu bilo koje druge imovine, uključujući i onu koja pripada društvu u cjelini i koja kao takva može biti izložena riziku ranjivosti, koji proizilazi iz upotrebe IKT-a (*Von Solms and Van Niekerk, 2013, 100*). Odnos ovih triju koncepta bezbjednosti ilustruje naredna slika.

Slika 2. Odnos između informacione, IKT i digitalne bezbjednosti



Izvor: Von Solms and Van Niekerk, 2013, 101.

Slično kao i kod digitalne bezbjednosti, tako i ekonomija digitalne bezbjednosti ima različite definicije. Tako prema Gordonu i Lebu ekonomija digitalne bezbjednosti je studija o tome kako organizacije određuju optimalno ulaganje u mjere zaštite vrijedne digitalne imovine uz balansiranje troškova i potencijalnih rizika (*Gordon and Loeb, 2002*). Nešto šire ekonomiju digitalne bezbjednosti posmatra Tajler Mur, koja je po njemu studija o tome kako ekonomski podsticaji oblikuju donošenje odluka o digitalnoj bezbjednosti, uključujući kako firme, pojedinci i vlade dodjeljuju resurse za ublažavanje digitalnih rizika i ulogu politike u rješavanju tržišnih neuspjeha (M*oore, 2010)*. Za Andersona i Mura ekonomija digitalne bezbjednosti ispituje kako pojedinci, organizacije i vlade raspoređuju resurse za zaštitu informacionih sistema, kao i podsticaje i kompromise koji su uključeni u donošenje odluka o digitalnoj bezbjednosti (*Anderson i Moore, 2006*).

4. LITERATURA

Može se reći da istraživanje ekonomije digitalne bezbjednosti počinje 2001. godine zapažanjem da loše usklađeni podsticaji objašnjavaju neuspjeh bezbjednosnih sistema barem jednako često kao i tehnički faktori (*Anderson, 2001*). Anderson ističe da se mnogi problemi u toj oblasti daju objasniti jezikom makroekonomije: mrežne eksternalije, asimetrične informacije, moralni hazard, nepovoljni izbor ili tragedija zajedničkog dobra. On je pošao od problema informacione bezbjednosti u bankama u zavisnosti od regulatornog okruženje. U SAD-u je banka bila obavezna da, kada se god klijenti žale, dokaže da li je klijent u pravu ili ne, dok je u Velikoj Britaniji

banka bila u pravu sve dok klijent ne dokaže suprotno. U zavisnosti od regulatornih zahtjeva, banke su imale različite podsticaje za ulaganje u tehnička rješenja za podizanje informacione bezbjednosti (*Anderson, 2001)*.

Gordon i Leb razvijaju model koji pokazuje da optimalno ulaganje u digitalnu bezbjednost ne mora nužno biti u korelaciji sa ukupnim nivoom ranjivosti ili vrijednošću informacione imovine. Umjesto toga, njihov ključni nalaz je da bi se firme trebale fokusirati na oblasti u kojima male investicije donose značajno smanjenje rizika, posebno za umjereno ranjive sisteme. Oni također tvrde da je optimalno ulaganje u digitalnu bezbjednost obično manje za 37% očekivanog gubitka. Ovaj rad je temelj u oblasti ekonomije informacione bezbjednosti, pružajući praktične uvide u balansiranje potrošnje na bezbjednost i upravljanja rizikom (*Gordon & Leb, 2002*).

Varian posmatra kolektivnu prirodu digitalne bezbjednosti i izazove osiguravanja pouzdanosti sistema u međusobno povezanim okruženjima. On ističe da pouzdanost sistema zavisi od najslabijih karika u mreži. Bezbjednosni izbori jedne strane mogu uticati na cijeli sistem, naglašavajući međusobno povezanu prirodu digitalne bezbjednosti. Dodatno, pojedinci ili organizacije mogu "besplatno koristiti" ulaganja drugih u poboljšanje bezbjednosti, posebno u zajedničkim sistemima. To se događa zato što se povećane prednosti često distribuiraju na sve korisnike, smanjujući podsticaj za individualne doprinose (*Varian, 2004*).

Anderson i drugi analiziraju stvarni ekonomski uticaj sajber kriminala, te kako se resursi troše na borbu protiv njega. Autori, između ostalog, zaključuju da su resursi u većem obimu usmjereni na rješavanje sajber kriminala nakon što se on dogodi, umjesto na smanjenje ranjivosti unaprijed. Troškovi sajber kriminala značajno variraju. Neki oblici sajber kriminala (npr. prevara u *online* bankarstvu) nameću direktne finansijske gubitke, dok drugi (npr. krađa intelektualne svojine) rezultiraju indirektnom, dugoročnom ekonomskom štetom. Mjere zašite izuzetno su skupe tako da često koštaju više od stvarnih gubitaka koje žele spriječiti (*Anderson et al, 2012*).

U *follow-up* studiji na istu temu iz 2019. godine, isti autori istražuju kako su troškovi kibernetičkog kriminala i strategije za njegovo rješavanje evoluirali od 2012. godine. Nalazi pokazuju da su finansijski gubici od tradicionalnog sajber kriminala (npr. prevarna plaćanja) i dalje značajni, indirektni troškovi (npr. oštećenje reputacije, zastoji u poslovanju) su značajno porasli. Značajno su se razvili novi tipovi napada. Nove prijetnje, kao što su *ransomware* i ranjivost „internet stvari", naglašavaju kako se sajber kriminal prilagođava novim tehnologijama. Također, sajber kriminal nesrazmjerno pogađa mala preduzeća i pojedince koji nemaju resurse za sprovođenje jakih bezbjednosnih mjera, te postoji rastuća potreba za međunarodnom saradnjom i snažnim politikama za borbu protiv globalne prirode sajber kriminala (*Anderson et al, 2012*).

Acemoglua, Malekiana i Ozdaglara *(2016*) istražuju kako struktura mreže i pojedinačne odluke o ulaganju u bezbjednost utiču na širenje rizika u međusobno povezanim sistemima (npr. sajber napadi, virusi) i razvijaju teorijski okvir za proučavanje ulaganja u bezbjednost i dinamiku zaraze u mrežama. Rad naglašava kritičnu ulogu mrežne strukture i strateških interakcija u određivanju sigurnosti mreže, te poziva na političke intervencije za rješavanje problema u koordinaciji slobodnog ponašanja, naglašavajući važnost usmjeravanja ulaganja u bezbjednost kako bi se ublažila zaraza i poboljšala ukupna otpornost mreže.

Asghari, van Eeten i Bauer (2016), ukazuju na to da digitalna bezbjednost nije samo tehnički problem, već složeno ekonomsko pitanje vođeno poticajima, eksternalijama itržišnom dinamikom. Efikasna rješenja zahtijevaju kombinaciju tehničkih mjera, intervencija politike i ekonomskih podsticaja za rješavanje tržišnih neuspjeha, usklađivanje interesa učesnika i podsticanje globalne saradnje. Vlade igraju ključnu ulogu u rješavanju tržišnih neuspjeha provođenjem standarda, ohrabrujući razmjenu informacija i podržavajući kolektivnu akciju. Autori naglašavaju važnost integracije ekonomskih teorija sa tehničkim znanjem za razvoj efikasnih strategija.

Mazaher, Kowalski i Øverby naglašavaju važnost integracije više različitih disciplina uključujući sociologiju, psihologiju, pravo, političke nauke i informatiku kako bi se osnažili donosioci odluka u evaluaciji i upravljanju situacijama, koje bi mogle dovesti do katastrofalnih posljedica i ugroziti održivost digitalnih ekosistema. Sistematskim razumijevanjem ekonomskih aspekata kibernetičke bezbjednosti, organizacije mogu donijeti informisane odluke kako bi poboljšale svoju otpornost na sajber prijetnje (*Mazaher, Kowalski and Øverby, 2021*). Isti autori razmatraju pitanje sajber bezbjednosti s aspekta javnih dobara. Autori tvrde da sajber bezbjednost ispoljava osobine i javnih i privatnih dobara, što dovodi do izazova u njenom obezbjeđivanju i upravljanju. Oni naglašavaju potrebu za nijansiranim razumijevanjem dvojne prirode sajber bezbjednosti kako bi se riješila pitanja poput nedovoljnog ulaganja i razvile učinkovite strategije za njeno unapređenje (*Mazaher, Kowalski & Øverby, 2022*).

U publikaciji Svjetske banke Cobos (*2024*) se ističe da su zemlje u razvoju sve podložnije sajber incidentima zbog faktora kao što su ograničeni resursi, neadekvatna infrastruktura, politička nestabilnost i brzo usvajanje digitalnih tehnologija. Sajber incidenti mogu dovesti do značajnih ekonomskih zastoja, poremetiti osnovne usluge i ometati društveni i ekonomski razvoj, potencijalno destabilizujući čitave ekonomije. Sektor digitalne bezbednosni u ovim regionima prepun je tržišnih neuspjeha, uključujući nisku svijest, rizike vezane za dobavljače i značajan nedostatak stručnjaka za sajber bezbjednost. Ova sveobuhvatna analiza naglašava kritičnu važnost jačanja okvira digitalne bezbjednosti na tržištima u razvoju kako bi se očuvala ekonomska stabilnost i promovisao održivi razvoj.

Detaljan pregled literature o podsticajima na ulaganja radi zaštite od sajber napada daju i Fedele i Rener (*2022*).

5. TRŽIŠTE

Tržište digitalne bezbjednosti pokazuje karakteristike i pozitivnih i negativnih eksternih efekata. Pozitivni i negativni eksterni efekti su loši iz ekonomske perspektive. S pozitivnim eksternalijama, obično ima manje dobrog nego što je poželjno. S negativnim eksternalijama, na kraju ima više loših stvari nego što je poželjno. Drugim riječima, u svijetu prepunom eksternalija, na kraju imamo manje ulaganja u bezbjednost od strane subjekata koji se ponašaju profesionalno i korektno i više štete od onih ignorantnih i zlonamjernih nego što bi bilo društveno optimalno.

5.1. Eksternalije

Nedovoljno bezbjednosti u sajber prostoru je očigledan primjer negativnog eksternog efekta. Kada se računari zaraze malicioznim softverom i regrutuju u *botnet*, šteta nije ograničena isključivo na taj kompromitovani računar. Kompjuteri sa malicioznim virusom mogu se koristiti u različite svrhe: za slanje neželjene pošte, za inficiranje drugih računara za pokretanje napada ili uskraćivanje usluge. U takvim slučajevima štetu snosi neko drugi, a ne vlasnik zaraženog računara. Posljedično, podsticaj za korisnike da obezbjede viši novo zaštite su umanjeni jer je ukupna šteta mnogo veća od one koju oni sami snose. Kao primjer mogu poslužiti elektroenergetske kompanije. Društveni gubici zbog kvara sistema upravljanja, kao što su produženi nestanci struje, premašuju finansijski gubitak pojedinačnog preduzeća u smislu izgubljenog prihoda. Privatni rizici s kojima se suočavaju takve kompanije su manji od društvenih rizika, što za rezultat ima nedovoljno ulaganje u zaštitu od socijalnih rizika (*Moore, 2010*).

Pozitivna eksternalija, kao posljedica tuđih radnji, korist je za treću stranu. Kada jedna firma ulaže u sajber bezbjednost koristi od toga imaju i drugi subjekti u sajber prostoru. Međutim, firma koja investira nije u mogućnosti da pobere sve koristi od svojih ulaganja. Za rezultat to na kraju ima manja ulaganja u sajber bezbjednost. Otkrivanje softverskih ranjivosti, također, stvara eksterne prednosti. Istraživači na polju sajber bezbjednosti naporno rade na pronalaženju od čega korist imaju i proizvođači antivirus softvera. Iako istraživači koji rade na poboljšanju softvera mogu ostvariti određene koristi za sebe, ipak nikada ne mogu požnjeti sve koristi od svojih napora. Kao rezultat toga, možemo očekivati manje ulaganja u otkrivanje ranjivosti antivirus programa od društveno optimalnog.

Razmjena informacija takođe pokazuje pozitivne eksternalije. Svaka firma, sa timom za obezbjeđenje, prati sajber napade na njihovu infrastrukturu, prirodno prikuplja podatke o prijetnjama koje bi mogle koristiti drugim organizacijama. Dijeljenje obavještajnih podataka o prijetnjama stvorilo bi pozitivne eksterne efekte.

5.2. Asimetrija informacija

Drugi ključni nedostatak tržišta digitalne bezbjednosti odnosi se na situaciju u kojoj su informacije nepotpune i neravnomjerno raspoređene među učesnicima na tržištu. Na primjer, kada kupci nemaju dovoljno informacija za pouzdano razlikovanje između proizvoda visokog kvaliteta od proizvoda niskog kvaliteta. Na primjer, pretplatnik koji želi kupiti pristup internetu možda neće moći razlikovati davaoce usluge koji imaju visoku sigurnost od onih sa manje striktnim pristupom. Zbog toga kupci nisu spremni da plate višu cijenu, što obeshrabruje privatne ponuđače.

Druga široka oblast u kojoj dolazi do asimetrije informacija proizilazi iz nedostatka podataka koji se odnose na incidente digitalne bezbjednosti. Kompanije više vole da ne otkrivaju kada trpe napad, pogotovo ako otkrivanje tih podataka nije zakonska obaveza. Dok neobjavljivanje može biti razumna strategija za pojedinačnu firmu, dotle su ostale firme na tržištu uskraćene za informacije koje bi im itekako mogle biti od koristi. Čak i kada firme dijele informacije o napadima, sklone su da izbjegavaju informacije o finansijskim posljedicama.

Kao rezultat očigledne asimetrije informacija imamo još dva klasična primjera tržišnog neuspjeha, a to su: negativna selekcija i moralni hazard. *Negativna selekcija* se može pojaviti na tržištu sajber osiguranja. Za osiguravača je veoma teško da napravi razliku između firmi na osnovu njihovih operativnih bezbjednosnih praksi. Nesigurne firme češće će kupuju sajber osiguranje, koje bi moglo izazvati veće premije i niže učešće nego inače. Drugi ishod asimetričnih informacija je *moralni hazard*. Ljudi mogu promijeniti svoje ponašanje ako im se pruži neka vrsta zaštite. Na primjer, u auto osiguranju, ljudi mogu voziti bezobzirnije ako su potpuno osigurani i imaju vrlo nisku franšizu jer znaju da će biti pokriveni. U praksi, moralni hazard nije bio značajno pitanje u kibernetičkoj bezbjednosti do sada, budući da osiguranje ne pokriva u potpunosti svu štetu koja proizilazi iz sajber napada. Moralni hazard može nastati i u drugim situacijama. Na primjer, u oblak okruženju, korisnici ne mogu dovoljno znati o bezbjednosti koje nudi provajder, dok provajderi ne mogu uvijek poznavati bezbjedonosne prakse svojih kupaca. U oba slučaja, svaka strana može biti u iskušenju da izbjegne svoje odgovornosti i da radi nesigurno.

Prisustvo tržišnog neuspjeha opravdava regulatornu intervenciju. Čak i kada su intervencije javne politike politički nepraktične, ukazivanje na postojanje tržišnog neuspjeha i dalje je korisno iz dva razloga. Prvo, to pomaže objasniti zašto imamo neoptimalna ulaganja u digitalnu bezbjednost. Drugo, moglo bi stvoriti mogućnosti i smjernice akterima da otkriju i riješe problem.

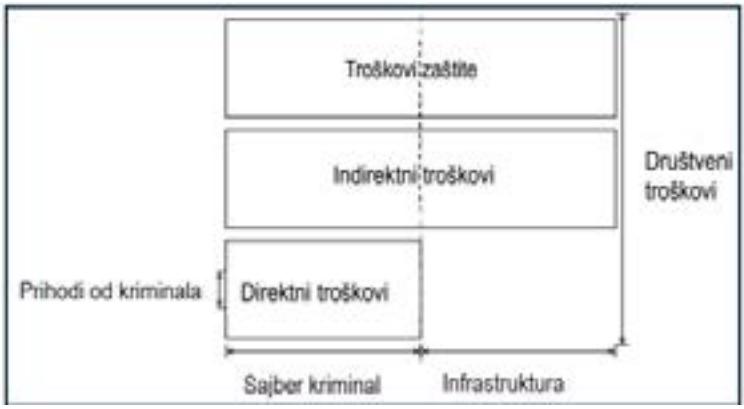
6. TROŠKOVI

Jedno od ključnih pitanja digitalne bezbjednosti jesu štete koje ti napadi prouzrokuju. Šteta može imati različite oblike, uključujući fizičke, psihičke, reputacijske, društvene, finansijske i slično. Kada ove štete možemo izraziti finansijski govorimo o troškovima sajber kriminala. Ponekad se ove štete mogu lako izraziti kao finansijski troškovi. Međutim, ukupne štete zbog sajber kriminala, praktično je nemoguće obuhvatiti. Bez obzira na podatke i procjene o visini troškova ili štetama prouzrokovanim sajber napadima, oni su definitivno ogromni. Pored toga, njihovo precizno utvrđivanje je praktično nemoguće, ne samo zbog raznovrsnosti štetnih uticaja i njihove disperzije na veliki broj subjekata nego i zbog tendencije pogođenih subjekata da ne objavljuju stvarne podatke o pričinjenim troškovima.

Troškovi od sajber nebezbjednosti se javljaju na različite načine. Tako određeni subjekti trpe direktni trošak, dok istovremeno mnogi drugi osjećaju indirektne troškove. Takođe, tu su i oportunitetni troškovi kao i društveni troškovi. Dio direktnih troškova su i prihodi koje sajber kriminalci ostvaruju. Indirektni troškovi uglavnom nadmašuju direktne finansijske gubitke žrtve napada (*Cobos, 2024, 49*).

Slika 3 daje okvir za analizu troškova sajber kriminala (*Anderson at al, 2012 i Andersson at all 2019*). Prihodi od kriminala su ukupni prihodi ostvareni kriminalnim aktivnostima, koje je takođe jako teško obuhvatiti i finansijski izraziti jer se kreću od uzimanja direktne otkupnine preko ucjene ili napada na bankovne račune, do koristi od upotrebe piratskog softvera i sl.

Slika 3. Troškovi napada u digitalnom okruženju



Izvor: Anderson at al, 2012

Direktan gubitak je finansijski gubitaki svake druge štete koju su žrtve osjetile kao posljedicu sajber kriminala. Primjeri uključuju novac povučen sa računa žrtava, troškovi da se ponovo aktivira račun korisnika, izgubljeno vrijeme zbog bavljenja neželjenim porukama, itd. Indirektni gubitak je vrijednost gubitaka i oportunitetnih troškova koje društvu nameće činjenica da se vrši određena vrsta sajber kriminala. Indirektni troškovi se generalno ne mogu pripisati pojedinačnim počiniocima ili žrtvama (*Anderson at al., 2012, Cobos and Cakir, 2024*).

Ključna razlika između direktnih i indirektnih troškova je u tome što direktni troškovi utiču na žrtvu, dok indirektne troškove snose subjekti koji nisu bili ciljane žrtve napada. Uobičajena je greška izjednačavanje indirektnih troškova sa nematerijalnim gubicima. Gubitak reputacije za firmu koja pretrpi zloupotrebu njenih podataka je direktan gubitak, iako je nematerijalan trošak. Nasuprot tome, ako vijesti o kršenju podataka koje ciljaju na maloprodaju natjeraju manje ljudi da kupuju zbog straha da će i njihove informacije biti otkrivene i zloupotrebljene, to bi bio indirektan trošak. Drugi primjeri uključuju gubitak povjerenja u internet bankarstvo, što dovodi do smanjenih prihoda od transakcionih naknada i većih troškova za održavanje, prodaja koju su propustili *online* trgovci kada njihovi mehanizmi za prevaru uzrokuju da odbiju korpe za kupovinu, smanjeno korištenje elektronskih usluga od strane građana bilo od strane kompanija ili vlada, otkazane operacije zbog nedostupnosti medicinskih usluga na mreži, napori za čišćenje mašine zaražene zlonamjernim softverom, itd. Indirektne troškove od sajber incidenata je teško kvantificirati i često se zanemaruju, iako mogu imati važan dugoročni uticaj na ekonomiju. Na primjer, Kamiya i drugi (*2021*) u analizi slučajeva u 75 firmi otkrivaju da indirektni troškovi (npr. troškovi sanacije, zakonske kazne i regulatorne kazne) su mnogo niži (1,2 milijarde USD) od ukupnog gubitka bogatstva dioničara (104 milijarde USD) nakon prijave zloupotrebe podataka.

Troškovi odbrane pokrivaju novac potrošen na prevenciju i kontrolu. Oni uključuju sigurnosne proizvode kao što su filteri za neželjenu poštu i antivirus, sigurnosne usluge koje se pružaju pojedincima, kao što je podizanje svijesti, sigurnosne usluge

koje se pružaju industriji, kao što su usluge uklanjanja web stranica, otkrivanje i oporavak prevara, provođenje zakona i oportunitetni troškovi kao što je propuštanje informacija kroz elektronsku poštu koja je pogrešno klasifikovana kao neželjena pošta. Kao i indirektni gubici, troškovi odbrane su uglavnom nezavisni od pojedinačnih počinilaca i žrtava pa čak i pojedinačnih vrsta sajber kriminala.

7. POLITIKE

Imajući prethodno u vidu jasno je da tržište neće osigurati optimalnu alokaciju u sektoru digitalne bezbjednosti, što znači da je neophodna intervencija vlasti kroz različite oblike politika. Međutim, to nikako ne znači da vlasti imaju mehanizme za efikasno rješavanje problema. Šta više i tu na površinu izbijaju i druge paradoksalne situacije. Vlasti žele da se kompanije i pojedinci obezbijede visokim nivoom vlastite zaštite. Međutim, često vlasti žele za sebe osigurati *backdoor* kako bi došli do informacija u cilju sprječavanja kriminalnih aktivnosti ili terorizma. Pored toga, malo ulaganja u digitalnu bezbjednost može značiti nizak nivo zaštite, dok visok nivo ulaganja može značiti da postoji nešto nedovoljno poznato ili pogrešno. Dalje, firme vrlo često ne žele da podaci o napadima na njih budu otkriveni i nastoje ih sakriti. Države bi trebalo da sarađuju na polju digitalne bezbjednosti, a često nemaju povjerenja jedne u druge. Isto tako, firme koje su zadužene da održavaju sajber prostor bezbjednim nisu istovremeno i one koje trpe štete od eventualnih napada (*De Bruijn and Janssen, 2017)*.

7.1. Regulativa

Prvi i najčešći oblik vladinog intervencionizma u slučaju zatajenja tržišta jeste regulisanje date oblasti dodjeljivanjem prava i odgovornosti. Naravno, treba svakako imati u vidu specifične okolnosti otkazivanja tržišta, te u tom smislu opet se oslanjati na ekonomske modele za alternativna rješenja, kao što je npr. Kouzova teorema u slučaju eksternalija ili pak dodjeljivanje kolektivnih prava u slučaju javnog dobra (*Kobayashi, 2009*).

Kouzova teorema kaže da ako su vlasnička prava dobro definisana, a troškovi transakcije niski, privatne strane mogu pregovarati o optimalnim rješenjima za eksternalije, bez potrebe za vladinom intervencijom.„Dakle, ako organizacije ili pojedinci jasno posjeduju odgovornost za digitalnu bezbjednost (npr. kroz ugovore ili zakone o odgovornosti), onda će oni pronaći najefikasniji način da smanje prijetnje od napada. Npr. preduzeće koje ima prijetnje od sajber napada može pregovarati sa pružaocem digitalnih usluga da obezbjedi bolje bezbjednosno filtriranje, umesto da se oslanja na vladine propise. Međutim, u praksi su transakcioni troškovi u slučaju digitalne bezbjednosti zaista visoki. Pregovaranje o sporazumima o digitalnoj bezbjednosti je složeno, posebno sa uključenim mnogim zainteresovanim stranama (vlade, preduzeća, provajderi, korisnici). Takođe, odgovornost za digitalnu bezbjednost često je nejasna, što otežava provođenje odgovornosti ili pak kompanije možda neće otkriti bezbjedonosne propuste, što otežava pregovore.

U takvoj situaciji, kada nije realno očekivati da privatni akteri na tržištu uspostave relacije, neophodno je da vlast interveniše dodjeljujući prava i odgovornosti. U tom slučaju se moraju svakako izbjeći mogućnosti zloupotrebe. I ovdje treba primijeniti

ekonomsku logiku, a u ovom slučaju to je princip tzv. *least cost avoider*, što znači da odgovornost treba pripisati onoj strani koja može spriječiti štetu uz najmanju cijenu. U kontekstu digitalne bezbjednosti primjena ovog principa upućuje na programere softvera i dobavljače internetskih usluga (ISP), a ne na krajnje korisnike. Ovi subjekti su u boljoj poziciji da efikasno sprovode sigurnosne mjere, čime se smanjuje ukupna učestalost digitalnih prijetnji, što treba da dovede do ekonomski efikasnijih praksi bezbjednosti.

Softver je uvijek imao greške, a mnogi sigurnosni incidenti visokog profila mogu se pratiti do ranjivosti u softveru. Neosporno je da mnogi programeri softvera ne slijede sigurne razvojne prakse ili ne preduzimaju dovoljno koraka za otkrivanje i uklanjanje ranjivosti prije finaliziranja koda. Vladinom regulativom bi trebalo odgovornost za siguran softver staviti na teret programerima jer su programeri softvera u najboljoj poziciji da poprave propuste uz najnižu cijenu. Eliminacija ranjivosti na njenom izvoru je jeftinija i efikasnija od očekivanja hiljada ili miliona kupaca koda za poduzimanje sigurnosnih mjera kako bi se blokirao uticaj napada koji iskorištavaju ranjivost. Dodjeljivanje odgovornosti programerima bi nesumnjivo podstaklo ulaganje u razvojne prakse sigurnog softvera. Međutim, protivnici softverske odgovornosti tvrde da je ipak nepravedno kriviti programere kada ranjivosti softvera budu otkrivene, jer bi softverska odgovornost mogla ometati inovacije, posebno u kontekstu razvoja besplatnog softvera otvorenog koda i da bi mnogo razvoja softvera otvorenog koda prestalo ako bi oni, pored ukupno uloženog truda, mogli biti odgovorni za greške. Dodatno, to bi moglo podići barijere za ulazak u razvoj softvera, što bi moglo obeshrabriti male firme za ulazak u ovaj biznis.

Zakonodavna regulativa igra ključnu ulogu u borbi protiv sajber napada, ali njena implementacija i dalje nije dovoljno efikasna. Naime, postoji nekoliko veoma ozbiljnih izazova koji dolaze sa strane izuzetno brzog razvoja tehnologija u ovoj oblasti: pitanja nadležnosti, veoma kompleksnog provođenja u praksi, balansiranja sa sigurnošću na jednoj i sa privatnošću i inovacijama na drugoj strani itd. Propisi se sporo donose i uglavnom kasne za digitalnim prijetnjama. Kadrovski resursi vlasti uglavnom nisu zadovoljavajući, kako u pripremi tako i u provođenju regulative. Digitalni napadi su vrlo često prekogranični, a međunarodni saradnja kao i međunarodni standardi nisu dovoljno razvijeni. Ne postoje globalni standardi za borbu protiv digitalnog kriminala. Zaštita privatnosti kao i zaštita poslovnih interesa kompanija stvara dodatne probleme. Strožiji nadzor u digitalnom prostoru izaziva podozrivost zbog mogućih zloupotreba i uticaja na privatnost građana. Istovremeno, zahtjevni propisi mogu predstavljati veliki teret za mala i srednja preduzeća.

7.2. Podizanje svijesti

Jedan od ozbiljnih problema, koji doprinosi većoj nebezbjednosti u digitalnom prostoru, je nedovoljno razumijevanje rizika, kao i nedovoljno poznavanje načina kako se zaštititi. Zaštita u digitalnom prostoru je problem za pojedince, organizacije i cijelo društvo. Kompanije preduzimaju različite mjere na podizanju svijesti, kao i na obučavanju svojih zaposlenih kako bi unaprijedili nivo zaštite. Međutim, digitalna bezbjednost kao društveni problem je zadatak za vladu. Pored različitih propisa kojima se utiče na nivo zaštite, jedna od ozbiljnih mjera vlasti trebaju biti kampanje

za podizanje svijesti o važnosti zaštite u digitalnom svijetu. Primarni cilj takvih kampanja treba biti da se utiče na usvajanje i praktikovanje bezbjednog ponašanja u digitalnom okruženju. Međutim, da bi kampanije zaista dale rezultate neophodno je da one budu ne samo informativne, nego i da ih korisnici prepoznaju kao bitne, da ih razumiju i da preduzmu djelovanje.

Postoji ogroman broj istraživanja, prije svega iz psihologije i srodnih područja, o uticaju na ljudsko ponašanje i promjenu ponašanja. Jedan od veoma obuhvatnih radova na tu temu je rad Dolana i drugih (*Dolan et al., 2010*) u kojem ukazuju na kritične faktore od uticaja na ljudsko ponašanje, kao što su: podsvijest, ego, afekt, emocije, norme, podsticaji itd. Međutim, kreatori politika digitalne bezbjednosti kao i eksperti u toj oblasti, često su kritikovani jer ne uspijevaju da objasne svoju poruku javnosti. Mada imaju dokaze, nisu uvijek u stanju da prenesu porukujavnosti i uvjere političare i kreatore politike da preduzmu akciju. Tipičan primjer je nauka o životnoj sredini, sa naučnicima koji nisu u stanju da ubijede kreatore politike u hitnost smanjenja emisije ugljenika. De Bruijn i Jansen (*2017*) predlažu koncept '*evidence-based framing*'. Ovaj koncept podrazumijeva da okvir komunikacije treba da bude zasnovan na činjenicama. Poruke koje su, na primjer, čisto emocionalne neće dugo živjeti, jer su podložne kontroli. Ljudi će, prije ili kasnije saznati da poruka nije tačna i prestaće da vjeruju pošiljaocu. Biće potrebno mnogo više truda da bi se povjerenje povratilo.

7.3. Objavljivanje podataka

Tendencija da se informacije o napadima ne objavljuju dokumentovana je u velikom broju istraživanja. Otkrivanje takvih informacija značajno smanjuje vrijednost dionica, prodaju i sl i na druge načine narušava reputaciju kompanije. Pad prodaje može se osjećati i do tri godine nakon incidenta, dok je pad dionica od preko 1% trenutan (*Kamiya et al., 2021*). Takva tendencija vodi ka asimetriji informacija o različitim ekonomskim efektima. Prije svega to daje pogrešnu sliku drugim kompanijama o obimu napada, njihovim karakteristikama i posljedicama, a što bi im svakako bilo od koristi u njihovom poslovanju, te razvijanju i primjeni različitih oblika zaštite. Što pouzdaniji podaci o sajber incidentima od naročite su koristi u sektoru osiguranja od sajber napada. Uprkos ozbiljnim i ogromnim problemima zbog sajber kriminala, tržište osiguranja u ovoj oblasti je i dalje nedovoljno razvijeno, a ne postojanje pouzdanih podataka o prijetnjama svakako značajno tome doprinosi. Osiguranje se zasniva na što je moguće pouzdanijim podacima iz prošlosti, kako bi mogli davati preporuke za zaštitu, te cijene uskladiti sa realnim rizicima. Da bi se ublažili efekti asimetričnih informacija, vlasti u mnogim zemljama donose propise o obaveznom otkrivanju podataka o sajber napadima. U tim zemljama tržište osiguranja je doživjelo značajniji rast tek nakon takvih propisa (*Nurse et al, 2020*). Propisi o obaveznom objavljivanju podataka o sajber napadima osim što će pomoći razvoju tržišta osiguranja i time povećati i samu zaštitu od sajber napada, takođe će pomoći drugim firmama da realno evaluiraju rizike i shodno njima preduzimaju adekvatne mjere. Dodatno, realni podaci će pomoći i podizanju svijesti o stvarnim prijetnjama.

7.4. Sertificiranje

Sertifikacija proizvoda namijenjenih zaštiti od napada u digitalnom prostoru nije nova. Već duže je u primjeni ali i dalje je izložena ozbiljnim nedostacima. Naime napadači sada nastoje da zloupotrijebe dokaze o originalnom, sertificiranom proizvodu, što je dodatni problem za vlasti da zaštite sam proces sertificiranja. Sa sve većim širenjem interneta stvari (IoT) ovaj način zaštite dobija na značaju. Naime, kupci i dalje evaluiraju proizvode na bazi kvaliteta, cijene i slično, a najmanje na bazi softverske zaštite. Poznat je napad tzv. *Mirai botneta* 2016. godine masovnim distribuiranim napadima uskraćivanja usluge (*DDoS*), od oko 600 000 uređaja. Stoga su mnoge zemlje, među njima je prvi bio Singapur (*CSA, 2021*), pokrenule programe sertificiranja softvera za internet stvari.

Pored sertifikacije proizvoda za digitalnu zaštitu, jednako ili čak više je bitno sertificiranje i samih procesa. U hiper umreženom svijetu danas, digitalna bezbjednost jedne kompanije, organizacije ili pojedinca u velikoj mjeri zavisi od nivoa zaštite njenih partnera u lancu snabdijevanja. Jedan od načina da se nezavisno provjere standardi zaštite drugih povezanih subjekata je ISO/IEC 27001, međunarodni standard za upravljanje digitalnom bezbjednošću (*Bird, 2023*). Standard su prvobitno zajedno objavile Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC) 2005. godine, a danas postoje i brojne priznate nacionalne varijante standarda. Organizacije koje ispunjavaju zahtjeve standarda mogu izabrati da budu sertificirane od strane akreditovanog sertifikacionog tijela nakon uspješnog završetka revizije. Naravno, ni sertificiranje procesa ne obezbjeđuje apsolutnu zaštitu. Naime, nisko postavljeni standardi neće obezbjediti dovoljnu zaštitu, dok visoko postavljeni standardi znače i više troškove za ispunjavanje zahtjeva i ne motivišu firme na njihovo uspostavljanje.

8. ZAKLJUČAK

Pitanje bezbjednosti u digitalnom prostoru nije samo tehničko pitanje. Bezbjednost nije uvijek rezultat dovoljne zaštite, odnosno ranjivosti sistema, nego vrlo često rezultat različitih poticaja učesnicima na tržištu digitalne bezbjednosti. Tehničke zaštite će biti više ili manje u zavisnosti od toga koliko su različiti akteri podstaknuti da preduzimaju adekvatne mjere. Posmatrano iz ugla ekonomije, tržište digitalne bezbjednosti ispoljava karakteristike sektora u kome tržište ne osigurava optimalnu alokaciju. Najčešći oblici neuspjeha tržišta su asimetrija informacija i eksterni efekti, bilo pozitivni ili negativni. I jedni i drugi su loši iz ekonomske perspektive. Pozitivni eksterni efekti znače podsticaj za manje ulaganja dok negativni efekti znače više loših stvari. Očigledno prisustvo tržišnog neuspjeha opravdava regulatornu intervenciju, koja prevashodno treba biti usmjerena u pravcu podizanja svijesti, obavezivanja na objavljivanje infomacija te propisivanje drugih oblika obavezujućeg postupanja.

Ekonomija digitalne bezbjednosti je novo područje ekonomskog istraživanja i u narednom periodu tek treba da dostigne svoj puni izraz. Dosadašnja istraživanja pokazala su da ekonomski pristup može biti od ogromne pomoći u unapređenju digitalne bezbjednosti, ali i ukazala na nove pravce istraživanja unutar ekonomske nauke. Potrebna su nova istraživanja iz domena upravljanja rizicima, u pogledu njihove uspješnije kvantifikacije i vrednovanja, kao i uticaja sajbernapada na kompanije

industrije i nacionalne ekonomije. Moralni hazard i nepovoljna selekcija svakako trebaju biti predmet istraživanja u okviru sajber osiguranja. Dodatno polje istraživanja otvara se i na polju bihejvioralne ekonomije, kao što su sklonost ka pretjeranoj samouvjerenosti, optimizmu, odnos prema riziku, te kako kreirati adekvatne politike u tom domenu (podsticanje na akciju, ohrabrivanje, obuka). Dalje, digitalna bezbjednost ima mnoga obilježja koja dozvoljavaju snažnu primjenu teorije igara, kao što su interakcija napadača i napadnutog, analiza digitalnog konflikta između država, razvijanje mehanizma saradnje kroz dijeljenje informacija itd.

LITERATURA

1. Anderson, Ross. 2001. Why information security is hard - an economic perspective. In *Seventeenth Annual Computer Security Applications Conference*, pp. 358–365.
2. Anderson, Ross and Tyler Moore. 2006. The Economics of Information Security. *Science,* 314, pp. 610-613.
3. Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Michael van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2012. Measuring the cost of cybercrime. In *11th Workshopon the Economics of Information Security (WEIS)*.
4. Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Carlos Ganan, Tom Grasso, Michael Levi, Tyler Moore, Stefan Savage, and Marie Vasek. 2019. Measuring the changing costof cybercrime. In *18th Workshop on the Economics of Information Security (WEIS)*.
5. Asghari, Hadi, Michel J.G. van Eeten, and Johannes M. Bauer. 2016."Economics of Cybersecurity". In *Handbook on the Economics of the Internet,* editedby Johannes M. Bauer & Michael Latzer. Cheltenham and Northampton: Edward Elgar, pp. 262-287.
6. Bird, Katie. 2023. New version of ISO/IEC 27001 to Better Tackle IT Security Risks, ISO, https://www.iso.org/news/2013/08/Ref1767.html.
7. Cobos, Vergara Estefania. 2024. Cybersecurity Economics for Emerging Markets, The World Bank, Washington, DC.
8. Cobos, Vergara Estefania and Cakir Selcen. 2024. A Review of the Economic Costs of Cyber Incidents, World Bank, Washington, DC.
9. CSA Singapore. 2021. Cybersecurity labelling scheme, 2021. https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.
10. De Bruijn, Hans and Marijn Janssen. 2017.Building cybersecurity awareness: The need for evidence-based framing strategies, *Government Information Quarterly, Vol.* 34, pp. 1–7.
11. Dolan Paul, Michael Hallsworth, David Halpern, Dominic King, Ivo Vlaev. 2010.*MINDSPACE: Influencing Behaviour Through Public Policy,*Institute for Government, Cabinet Office.
12. Fedele, Alessandro and Cristian Roner. 2022. Dangerous games: A literature review oncybersecurity investments, *Journal of Economic Surveys*, Vol. 36, pp. 157–187.
13. Gordon, A. Lawrence andMartin P. Loeb. 2002. The economics of information security investment, *ACM Transactions on Information and System Security*, Vol. 5, No. 4, November, pp. 438-457.
14. Gordon, A. Lawrence, Martin P. Loeb and Lei Zhou. 2016. Investing in Cybersecurity: Insights from the Gordo-Loeb Model. *Journal of Information Security*, **7**, pp. 49-59.
15. IBM. 2024. Cost of a Data Breach Report 2024, IBM, Armonk, New York.
16. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. 2021. 'Risk management, firm-reputation, and the impact of successful cyberattacks on target firms', *Journal of Financial Economics,* Vol. 139, pp. 719-749.
17. Kelly, Douglas. 2017. "The Economics of Cybersecurity", in *Proceedings of the 12th InternationalConference on Cyber Warfare and Security*, edited by A. R. Bryant, J. R. Lopez, and R. F. Mills, Academic Conferences International Limited.

18. Kianpour, Mazaher, Stewart James Kowalski and Harald Øverby. 2021. Systematically understanding Cybersecurity Economics: A Survey. *Sustainability13*, 13677.
19. Kianpour, Mazaher, Stewart James Kowalski and Harald Øverby. 2022. Advancing the concept of cybersecurity as a public good, *Simulation Modelling Practice and Theory,* 116, 102493.
20. Kobayashi, H. Bruce. 2006. An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods, *Supreme Court Economic Review*, Vol. 14, pp. 261-280.
21. Moore, Tyler. 2010. The Economics of Cybersecurity: Principles and Policy Options *International Journal of Critical Infrastructure Protection,* Volume 3, Issues 3-4, pp. 103-117,
22. Nurse R. C. Jason, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, andSadie Creese. 2020. The data that drives cyber insurance: A study into the underwriting andclaims processes. In *2020 International Conference on Cyber Situational Awareness, DataAnalytics and Assessment (CyberSA)*, pp. 1–8.
23. Solms, R. Von, Van J. Niekerk. 2013. From information security to cyber security. *Computer Security,* Vol. 38, pp. 97–102.